JAIME EVARISTO
EDUARDO PERDIGÃO

INTRODUÇÃO À ÁLGEBRA ABSTRATA

- A linguagem matemática
- Construção axiomática do conjunto dos naturais
- Estruturas algébricas: anéis, domínios, corpos
- Construção axiomática e por definição do conjunto dos inteiros
- Propriedades dos números inteiros
- Construção dos conjuntos dos racionais e dos reais
- Aplicações à Computação: armazenamento de caracteres, armazenamento de números inteiros, divisão por dois, algoritmo rápido para potências, eficiência do Algoritmo de Euclides
- . . .

Jaime Evaristo
Mestre em Matemática

Eduardo Perdigão
Doutor em Matemática

Introdução à Álgebra Abstrata

Terceira Edição
Formato e-book
Maceió, outubro 2020

Prefácio (da primeira edição)

Quem atua em processos de ensino/aprendizagem de Matemática, fatalmente, já teve de ouvir a pergunta: *por que se estuda Matemática?* Além do fato de ela permitir o exercício de algumas ações práticas do cidadão (como o gerenciamento de suas finanças, por exemplo) e a compreensão de alguns fenômenos relativos à sociedade (como a evolução de uma população, por exemplo), a Matemática fornece uma poderosa ferramenta simbólica que serve de suporte ao pensamento humano, explicitando intensidades, relações entre grandezas e relações lógicas, sendo, por esse motivo e por excelência, a linguagem da Ciência. Além disso, o ato de estudar Matemática desenvolve o raciocínio do estudante e isso permite que ele seja capaz de compreender com mais facilidade os conceitos de outros ramos do conhecimento humano e as interrelações entre esses conceitos. A Álgebra Abstrata, estabelecendo os seus fundamentos, é onde a linguagem Matemática é definida e onde a compreensão dos conceitos, pelos seus níveis de abstração, requer o desenvolvimento de raciocínios que ajudarão na aprendizagem de outras ciências.

O escopo deste livro é servir de livro-texto para uma disciplina inicial de Álgebra Abstrata e foi concebido de tal forma que não exige nenhum conhecimento anterior, podendo também ser lido por estudantes ou profissionais de outras áreas que pretendam ter uma ideia do que é Matemática. Para que o seu conteúdo seja autossuficiente, o livro contém a construção de todos os conjuntos numéricos, com exceção do Conjunto dos Números Complexos. Além disso, e considerando a sua importância nas aplicações, o livro apresenta um estudo detalhado dos números inteiros, discutindo suas propriedades, números primos, fatoração etc.

O livro também apresenta uma aplicação muito importante da álgebra abstrata à informática e uma amostra (naturalmente, em um exemplo bem simples) de como se pode fazer pesquisa em Matemática, apresentando definições de conjuntos e de funções que não constam da literatura.

Uma parte importante do livro são seus exercícios propostos. Alguns têm o objetivo de fixar a aprendizagem; outros são acréscimos à teoria exposta. O estudante deve tentar exaustivamente solucionar todos eles, não procurando ver a solução que se apresenta ao menor sinal de

dificuldade. O esforço que se realiza ao se tentar resolver um problema de Matemática, bem sucedido ou não, é muito importante para o processo da aprendizagem.

Os autores agradecem a Elizamar Batista dos Santos e a Alcineu Bazilio Rodrigues Júnior pela colaboração na digitação do livro e, antecipadamente, a todo leitor, estudante ou professor, que enviar qualquer crítica ou sugestão para jaime@ic.ufal.br ou para perdigao@mat.ufal.br. Os autores também agradecem ao Professor Antônio Carlos Marques da Silva que emitiu parecer sobre o material do livro para apreciação do Conselho Editorial da EDUFAL e ao Professor Eraldo Ferraz, diretor da editora, pelo empenho em publicar esta obra.

Maceió, julho de 2002
Jaime Evaristo
Eduardo Perdigão

Prefácio (da segunda edição)

Esta segunda edição é uma revisão muito acurada do texto original, incluindo correções de erros de digitação e erros de conceitos, destaques de alguns conteúdos como novas seções, apresentação de novas demonstrações de proposições matemáticas e introdução, exclusão e reordenação de exercícios propostos.

Além de contar com as percepções de erros e sugestões dos meus alunos que utilizaram a primeira edição no período compreendido entre de 2002 e 2008, esta edição teve importante participação dos alunos do curso de Ciência da Computação e de Engenharia de Computação da Universidade Federal de Alagoas Ailton Felix de Lima Filho, Bruno Normande Lins, Emanuella Toledo Lopes, Erique Cavalcante Medeiros da Hora, Fernando Henrique Tavares Lima da Silva, Jônathas Magalhães Nunes, Kaio Cezar da Silva Oliveira, Michael Denison Lemos Martins, Michel Alves dos Santos, Wylken dos Santos Machado, Yuri Soares Brandão Vanderlei, Clenisson Calaça Cavalcante Gomes, Dielson Sales de Carvalho, Erick Diego Odilon de Lima, Everton Hercilio do Nascimento Santos, Fernanda Silva Bezerra de Albuquerque, Rafael Fernandes Pugliese de Moraes, Rafael Henrique Santos Rocha, Daniel Duarte Baracho, Diogo Felipe da Costa Carvalho, Gilton José Ferreira da Silva, Joao Pedro Brazil Silva, Kalline Nascimento da Nóbrega, Revanes Rocha Lins, Rodrigo Rozendo Bastos, Samuel das Chagas Macena, Sergio Rafael Tenório da Silva, Thiago Luiz Cavalcante Peixoto, Rafaele Sthefane Barbosa Oliveira, Lucas Lins de Lima, Fernando dos Santos Costa, Francisco Victor dos Santos Correia, Luciano de Melo Silva, Gustavo de Oliveira Gama, Ivo Gabriel Guedes Alves, Yuri Santos Nunes, Iago Barboza de Souza, Ísis de Sá Araújo Costa, Michael Gusmão Buarque Aliendro, Nicole Goulart Fonseca Acioli, Layane Nascimento de Araújo, Laysa Silva de Paula, Paulo Henrique Félix Barbosa, Evérton Borges da Silva, Gustavo de Oliveira Gama, Luciano Menezes da Costa, Tamirys Coelho de Oliveira Pino, Daniel San Ferreira da Rocha e João Gabriel Gama. Sem demérito para os demais, gostaria de ressaltar a participação muito efetiva dos alunos Gerlivaldo Felinto da Silva e Leonildo de Mello Nascimento. Também gostaríamos de agradecer as participações do Professor Alcino Dall'Igna, que propiciou a inclusão da seção “Divisão

por 2 em computadores", e de Pedro Roberto de Lima, que nos indicou um erro (grave) na bibliografia. Em 2013, os alunos Pedro Ivo Mariano de Oliveira Barros e Edvonaldo Horácio perceberam erros sutis em demonstrações.

Sendo uma edição digital, correções e inclusões no texto podem ser feitas a qualquer momento. Assim, os autores agradecem a participação dos leitores no sentido da melhoria do livro (inclusive, com a inclusão de novos exercícios) e prometem registrar no livro essas participações. Toda e qualquer observação deve ser encaminhada para jaime@ic.ufal.br, com o assunto LIVRO INTRODUÇÃO À ÁLGEBRA ABSTRATA.

Maceió, dezembro de 2013
Jaime Evaristo
Eduardo Perdigão

Prefácio (da atual edição)

Nesta edição, ampliamos a discursão sobre a linguagem matemática, tentamos diminuir as questões envolvendo deslizes da língua portuguesa, destacamos como um capítulo a principal aplicação do livro (criptografia RSA), atualizamos as informações sobre os números primos e apresentamos maiores detalhes do estudo dos números reais. Além disso, foram incluídos novos exercícios e reformulados alguns deles. Também foi disponibilizado, em livro à parte, um manual com propostas de soluções (escritas de forma a mais didática possível) de todos os exercícios do livro. Ao publicar o manual de soluções (contém também os enunciados) à parte, tivemos o objetivo de não "engrossar" mais o livro que já tem mais de trezentas páginas (o manual de soluções tem mais de cem páginas).

Os dois primeiros capítulos desta edição contaram com uma leitura revisional do Professor Elthon Oliveira, da Universidade Federal de Alagoas, ao qual os autores agradecem.

Maceió, outubro de 2020
Jaime Evaristo
Eduardo Perdigão

Sumário

1. Conjuntos e Funções

1.1 A linguagem matemática

As duas primeiras acepções do vocábulo LINGUAGEM apresentadas no dicionário Michaelis (https://michaelis.uol.com.br, acesso em 08/06/2020) indicam:

1 LING Faculdade que tem todo homem de comunicar seus pensamentos e sentimentos.

2 LING Conjunto de sinais falados, escritos ou gesticulados de que se serve o homem para exprimir esses pensamentos e sentimentos.

De um modo simplificado (suficiente para o nosso propósito), os sinais falados são os fonemas, que constituem a linguagem falada, e os sinais escritos são as letras que constituem as palavras, que, por sua vez, constituem a linguagem escrita.

Ainda de acordo com o Michaelis, o "conjunto de palavras ou signos vocais e regras combinatórias estabelecidas, de que fazem uso os membros de uma comunidade para se comunicar e interagir" é chamado *língua* ou *idioma,* os quais podem ser entendidos também como o "sistema de comunicação oral e escrita de um país, estado ou território". Exemplo óbvio: as leis do Brasil definem a Língua

Portuguesa como uma das línguas oficiais do país (a outra língua oficial é a LIBRAS, Língua Brasileira de Sinais).

Para denominar seus "achados", o desenvolvimento de uma ciência (ou de qualquer campo da atividade humana) exige a criação de novos vocábulos ou a utilização de palavras (às vezes, uma locução) de uma língua já estabelecida, com significados próprios. Usando a Matemática e a Física, respectivamente, *hipotenusa* e *entropia* são exemplos do primeiro caso e *operação* e *buraco negro*, do segundo (*operação* no "sentido matemático" será exaustivamente estudada ainda neste capítulo). Além de criar vocábulos ou utilizar palavras de um idioma com significados seus, a Matemática também cria expressões (no sentido gramatical do termo) para expressar suas ideias. Nesse caso, quase sempre, cria signos para representá-las. Constitui-se então a *linguagem matemática*, dotada de precisão e rigor, e rica em vocábulos próprios, em utilização de palavras com significados próprios, em expressões com sentidos próprios e, ao contrário de outras ciências, em símbolos para facilitar a escrita dos textos.

Corroborando o que foi dito no prefácio da primeira edição, a leitura deste livro e a aquisição dos conhecimentos que ele pretende desenvolver não exigem nenhum conhecimento prévio da linguagem matemática: todos os vocábulos da linguagem serão definidos ou

conceituados, todas as expressões serão explicadas, todos os signos serão estabelecidos. Ou seja, partiremos do zero! Vamos precisar apenas de pequenas concessões: algumas vezes, para definir um *ente matemático* (ou seja, um objeto utilizado na Matemática, um objeto "da Matemática") precisamos nos referir a algum conceito da língua portuguesa. Nesse caso, utilizaremos a expressão "no sentido usual do termo".

1.2 Entes primitivos

Recorrendo agora a outro dicionário, o Dicionário Aurélio estabelece que *definir* é *enunciar os atributos essenciais e específicos de (uma coisa), de modo que a torne inconfundível com outra*. Para que o objetivo de uma definição seja atingido, devem ser observados dois aspectos: uma definição só pode conter termos que foram definidos previamente e uma definição de um objeto não pode conter um termo cuja definição contenha referência ao próprio objeto. Um exemplo claro de "definições" que pecam em relação ao segundo aspecto levantado são as que aparecem em livros da educação básica:

i) Um *ponto* é a interseção de duas *retas*.

ii) Uma *reta* é um conjunto de *pontos alinhados*.

Com essas "definições", para se entender o que é um *ponto* é

necessário saber o que é uma *reta* e para compreender o que é uma *reta* é indispensável saber o que é um *ponto* e o que são *pontos alinhados*.

Um exemplo do primeiro aspecto levantado na discussão do que é *definir* é o que se encontra em alguns livros de Matemática como "definição" de *conjunto*: *conjunto é uma coleção de objetos*. O problema agora é que essa "definição" dá margem à seguinte pergunta: e o que é uma *coleção de objetos*? A resposta não poderia ser *conjunto* pois cairíamos no outro problema.

Evidentemente, a exigência de que uma definição somente contenha termos definidos previamente gera um "vai para trás" infinito, no sentido usual do termo. Uma solução para esse "vai para trás infinito" (talvez seja a única saída!) é se adotar "pontos de partida" sem definições. Na Física, os "pontos de partida" são chamados *grandezas primitivas*: o *tempo*, a *distância* e a *massa* são exemplos. Na Matemática, os "pontos de partida" são chamados *entes primitivos*: *ponto*, *reta* e *plano* são entes primitivos da Geometria Euclidiana, parte da Matemática que se começa a estudar na Educação Básica.

Na Física, a partir das grandezas primitivas pode-se definir outras grandezas, as quais podem ser utilizadas para se definir outras grandezas e, assim, sucessivamente. Por exemplo, a partir das

grandezas primitivas distância e tempo define-se *velocidade* como o quociente entre a *distância* percorrida e o *tempo* gasto para percorrê-la; a partir da velocidade e do tempo define-se *aceleração* como o quociente entre a variação da velocidade e o tempo em que ocorreu essa variação. Na Matemática ... Ainda não temos conhecimentos suficientes para apresentar um exemplo de um objeto definível.

Uma questão inicial para se utilizar um ente primitivo é se estabelecer sua compreensão (se tal objeto não é definido, como ter uma ideia do que ele é!). Quando ministrávamos aulas de Geometria, utilizávamos a seguinte estratégia para transmitir a ideia de ponto. Pedia para que os alunos imaginassem tocar uma folha de papel com um lápis com uma ponta bem fina e, após a realização abstrata da ação, dizia, gravemente, isto não é um ponto! Pedia para os alunos afinarem mais a ponta do lápis e tocassem novamente a folha de papel e repetia o anúncio: isto ainda não um ponto. Pedia para os alunos afinarem mais a ponta do lápis, tocar a folha de papel e anunciava mais uma vez: isto ainda não é um ponto ...

1.3 Conjuntos

Recorrendo mais uma vez ao Dicionário Michaelis, encontramos as seguintes acepções de conjunto:

conjunto
adj
1 Diz-se daquilo que ocorre em simultaneidade ou concomitância com outro elemento qualquer, a ele se somando em estreita relação; agregado, somado, reunido, ligado.
2 Que se localiza em lugar próximo; anexo, contíguo, adjacente.
sm
1 Reunião dos elementos ou das partes que constituem um todo.
2 Agrupamento de pessoas envolvidas em uma atividade comum; equipe, time, corpo.
3 Grupo de artistas (cantores, dançarinos, músicos etc.) com formação estável que interpreta ou executa a mesma composição; companhia, banda, coro etc.
4 Coleção ou reunião de objetos, utensílios etc. que apresentam uma característica comum ou se destinam à mesma finalidade.
5 A soma total de vários elementos; totalidade.
6 Resultado ou eficácia que resulta do trabalho produzido coletivamente, com a soma dos esforços dos componentes de um grupo, associação, escola etc.; unidade.
7 Traje, feminino ou masculino (este geralmente esportivo), composto de peças combinadas para ser usadas juntas: calças e blazer, saia e casaco, vestido e casaco etc.; costume, terninho.
8 MAT Conceito primitivo, de difícil precisão e definição, que corresponde à ideia intuitiva de reunião, coleção ou agrupamento de objetos ou elementos, determinados e diferenciáveis, próprios da realidade exterior ou oriundos das construções do pensamento.

Ou seja, na língua portuguesa o vocábulo *conjunto* tem muitos

significados! Como ela mesmo indica, para a Linguagem Matemática nos interessa a última acepção listada, só que de uma forma mais simples. A Matemática não considera *conjunto* como um conceito "de difícil precisão e definição". Para a Matemática, da mesma maneira que ponto, reta e plano, *conjunto* é um ente primitivo (portanto, não é definido, para lembrar), sendo entendido como uma reunião, coleção ou agrupamento de objetos, todos esses vocábulos sendo utilizados nos seus sentidos usuais. Os objetos que compõem a coleção que está sendo considerada um conjunto são chamados *elementos* do conjunto e dizemos que o elemento *pertence* ao conjunto. Dessa forma, estabelecemos, de forma também *primitiva*, uma relação (no sentido usual do termo) entre elementos e conjuntos, chamada de *pertinência*. Se convencionarmos, de um modo geral, representar conjuntos por letras maiúsculas e seus elementos por letras minúsculas, indicaremos a relação de pertinência de um objeto x a um conjunto A por $x \in A$, expressão que é lida "*x pertence a A*". Naturalmente, se um objeto não está na coleção que se está considerando como um conjunto, dizemos que tal objeto *não pertence* ao tal conjunto, sendo utilizado o símbolo $\notin$ para negar a relação de pertinência.

Introduzido o conceito primitivo de conjunto e utilizando os entes primitivos ponto e plano e a grandeza primitiva distância, podemos apresentar um exemplo de um objeto da Matemática que é

definido: dados um plano α, um ponto p do plano α e um número real r, a *circunferência* contida no plano α, de *centro* p e *raio* r é o conjunto dos pontos do plano α situados a uma distância r do ponto p. (Observe que abrimos uma concessão em relação à exigência de que uma definição só contenha termos definidos anteriormente: não definimos ainda o que é número real; isso será feito no capítulo 10).

1.4 Igualdade

Seguindo a linha da seção anterior, uma consulta ao significado de *igualdade* no Google (acesso em 14/06/2020) resulta em algumas respostas, como, por exemplo:

a) Página do Google (adaptada)

igualdade
substantivo feminino
1. fato de não apresentar diferença quantitativa.
2. fato de não se apresentar diferença de qualidade ou valor, ou de, numa comparação, mostrarem-se as mesmas proporções, dimensões, naturezas, aparências, intensidades; uniformidade; paridade; estabilidade.

b) Dicionário Online de Português

Significado de Igualdade
substantivo feminino
1. Falta de diferenças; de mesmo valor ou de acordo com mesmo ponto de vista, quando comparados com outra coisa ou pessoa: igualdade racial; igualdade salarial; igualdade de vagas.

2. Princípio de acordo com o qual todos os indivíduos estão sujeitos à lei e possuem direitos e deveres; justiça.

3. [Matemática] Relação entre grandezas de mesmo valor; a fórmula que demonstra essa relação.

4. Uniformidade, continuidade: igualdade de ânimo.

Infelizmente (ou felizmente, dependendo do ponto de vista), ao contrário do que vimos sobre conjuntos, nenhum dos significados encontrados satisfaz os interesses da Matemática, inclusive o subitem 3 do item (b) (o que seria "de mesmo valor"?). Entendemos que não há outra solução de considerar *igualdade* como um conceito primitivo no sentido de que quando ficar estabelecido que dois objetos matemáticos são *iguais* eles passam a ser considerados o mesmo objeto.

A igualdade de dois objetos é representada pelo símbolo = e se dois objetos não são iguais (e, portanto, não podem ser considerados o mesmo objeto) dizemos que eles são *diferentes*, indicando este fato pelo símbolo ≠. Por exemplo, no alfabeto da língua portuguesa, B e b são consideradas a mesma letra, e daí podemos escrever B = b, ao passo que b e k não são a mesma letra e escrevemos b ≠ k. (O alfabeto da língua portuguesa será utilizado em vários exemplos e será referido apenas por *alfabeto*).

Vamos admitir primitivamente que as seguintes afirmações são verdadeiras:

i) Todo objeto é igual a ele mesmo: $a = a$, qualquer que seja o objeto a.

ii) Se um objeto é igual a outro, este é igual àquele: se $a = b$, então $b = a$;

iii) Dois objetos iguais a um terceiro objeto são iguais entre si: se $a = b$ e $b = c$, então $a = c$.

A terceira afirmação vai permitir que escrevamos $a = b = c$ quando tratarmos de três elementos que serão considerados o mesmo elemento.

Como igualdade em Matemática é um conceito primitivo, toda vez que se introduz (primitivamente ou por definição) um ente matemático é necessário se estabelecer quando dois representantes desse ente serão considerados iguais. Por exemplo, introduzido o ente matemático conjunto, devemos estabelecer quando dois conjuntos serão ditos iguais, o que será feito na seção 1.7.

1.5 Subconjuntos

Sejam A e B dois conjuntos. Por definição, dizemos que o conjunto A é *subconjunto* do conjunto B se todo elemento de A é também elemento de B. Quando isto acontece, escrevemos $A \subset B$, que é lido *A é subconjunto de B* ou *A está contido* em B. Nesse caso,

também podemos escrever $B \supset A$, que é lido *B contém A*. A negação de $A \subset B$ é indicada por $A \not\subset B$ (*A* não é subconjunto de *B* ou *A* não está contido em *B*) e é verdadeira se *A* possuir pelo menos um elemento que não pertença a *B*.

As seguintes afirmações são claramente verdadeiras:

1. $A \subset A$, qualquer que seja o conjunto *A*.

2. Se $A \subset B$ e $B \subset C$, então $A \subset C$, quaisquer que sejam os conjuntos *A*, *B* e *C*.

A afirmação 1 é justificada pelo fato óbvio de que todo elemento do conjunto *A* é elemento do conjunto *A*. A afirmação 2 se justifica com o seguinte argumento: de $A \subset B$ segue que todo elemento de *A* é elemento de *B*; porém, como $B \subset C$, temos que todo elemento de *B* é elemento de *C*. Logo todo elemento do conjunto *A* é elemento do conjunto *C*, mostrando que $A \subset C$.

Uma afirmação verdadeira a respeito de um ente matemático é chamada *propriedade* daquele ente. Um argumento que justifica a veracidade de uma propriedade é chamado *demonstração* ou *prova* daquela propriedade. Na seção anterior, admitimos primitivamente três propriedades da igualdade.

Observe que se *A* e *B* são dois conjuntos tais que $A \subset B$, pode ocorrer que se tenha $A = B$. Quando dois conjuntos *A* e *B* são tais que

$A \subset B$ e $A \neq$ B, dizemos que A é *subconjunto próprio* de B (evidente, ainda falta aprendermos o que significa $A \subset B$.

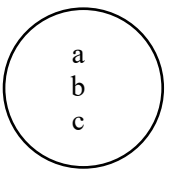
1.6 Uma representação de conjuntos

Uma das formas de se representar um conjunto é exibir os seus elementos entre chaves {}. Por exemplo, $A = \{a, b, c\}$ é o conjunto das três primeiras letras do alfabeto latino. O conjunto das letras do alfabeto pode ser indicado por $A = \{a, b, c, ..., z\}$, onde as reticências são utilizadas para simplificação e substituem as letras de d a y. O uso de reticências para subentender alguns (às vezes muitos) elementos de um conjunto só é possível se os elementos do conjunto obedecerem a uma ordenação (no sentido usual do termo) previamente conhecida. Quando isto não acontece, as únicas alternativas são explicitar todos os elementos do conjunto ou definir o conjunto por uma expressão da língua portuguesa. Um exemplo de um desses conjuntos é o conjunto dos caracteres da língua portuguesa, que possui letras maiúsculas e minúsculas, dígitos, letras acentuadas, caracteres de pontuação etc.

Os elementos de um conjunto podem ser outros conjuntos. Por exemplo, o alfabeto pode ser visto como um conjunto que possui dois conjuntos: o conjunto das vogais e o conjunto das consoantes. Do mesmo modo, podemos pensar em conjuntos como $B = \{\{a\}, \{a, b\},$

{a, b, c}, ..., {a, b, c, ..., z}}.

Outra forma de representar conjuntos é dispor os seus elementos dentro de uma circunferência (ou uma linha curva fechada, nos sentidos usuais dos termos), forma que é chamada *diagrama de Venn*. Por exemplo, o diagrama de Venn do conjunto A = {a, b, c} é simplesmente



Os diagramas de Venn, mesmo com toda simplicidade, propiciam uma técnica interessante para resolver questões envolvendo pesquisas de opinião. Um exemplo do uso dessa técnica será visto no capítulo 2.

1.7 Igualdade de conjuntos

Como estabelecemos na seção 1.4, a igualdade de objetos matemáticos é um conceito primitivo: quando se estabelece que dois objetos são iguais, eles são considerados o mesmo objeto. Nessa seção também ficou dito que quando um ente matemático for introduzido, deve-se definir quando dois desses entese serão iguais.

No caso de conjuntos, a definição de igualdade é muito

simples e muito natural: dois conjuntos são *iguais* se eles possuem os mesmos elementos. Por exemplo, os conjuntos $A = \{a, b, c\}$ e $B = \{c, b, a\}$ são iguais. Os conjuntos $A = \{a, b, c\}$ e $C = \{a, b\}$ são diferentes.

Essa definição mostra que na representação de um conjunto pela exibição dos seus elementos a ordem (no sentido usual do termo) com que os elementos são exibidos não é utilizada para discriminar um conjunto (e justifica a representação pelos diagramas de Vem). Assim os conjuntos $A = \{x, k, m\}$ e $B = \{m, x, k\}$ são iguais. A repetição da exibição de um elemento também não implica a diferenciação de um conjunto: os conjuntos $A = \{a, b, c\}$ e $B = \{a, b, a, c, b\}$ também são iguais.

Vale observar que se dois conjuntos são iguais (se possuem os mesmos elementos!), é evidente que todo elemento do primeiro é elemento do segundo e, reciprocamente, todo elemento do segundo é elemento do primeiro. Ou seja, se $A = B$, então $A \subset B$ e $B \subset A$. Por outro lado, se $A \subset B$ e $B \subset A$, então todo elemento de A é elemento de B e todo elemento de B é elemento de A, o que mostra que $A = B$. Ou seja, se $A \subset B$ e $B \subset A$, então $A = B$. (Vamos mostrar mais para frente que a linguagem matemática tem recursos para facilitar a escrita das conclusões desse parágrafo).

1.8 Par ordenado

Para podermos definir um ente matemático (chamado *função*) fundamental para todas áreas da Matemática, precisamos trabalhar com pares de elementos, considerados em uma ordem preestabelecida. Daí necessitarmos da seguinte definição. Sejam A e B dois conjuntos e a e b elementos de A e de B, respectivamente. O *par ordenado a b*, indicado por (a, b), é o conjunto $\{\{a\}, \{a, b\}\}$, ou seja, (a, b), é o conjunto $\{\{a\}, \{a, b\}\}$. Vale observar que, se os conjuntos A e B forem iguais, podemos ter par do tipo (a, a). Evidentemente, $(a, a) = \{\{a\}, \{a, a\}\} = \{\{a\}, \{a\}\} = \{\{a\}\}$.

Observe que se A e B são dois conjuntos, $a, j \in A$ e $b, k \in B$ e $(a, b) = (j, k)$, então $a = j$ e $b = k$. De fato, de $(a, b) = (j, k)$ segue que:

i) Se $a = b$, temos que os conjuntos $X = \{\{a\}\}$ e $Y = \{\{j\}, \{j, k\}\}$ são iguais o que só acontece se $j = k = a$.

ii) Se $a \neq b$, temos $\{j\} \neq \{a, b\}$ e a igualdade dos conjuntos $X = \{\{a\}, \{a, b\}\}$ e $Y = \{\{j\}, \{j, k\}\}$ implica $\{a\} = \{j\}$ e $\{a, b\} = \{j, k\}$ o que acarreta $a = j$ e $b = k$.

A veracidade dessa afirmação, além de justificar a denominação *par ordenado*, permite que se distinga os elementos que compõem o par, já que $(a, b) = \{\{a\}, \{a, b\}\}$ e $(b, a) = \{\{b\}, \{b, a\}\}$: no par (x, y), x é a *primeira componente* e y é a *segunda componente*.

Os autores concordam com o leitor que achar um pouco abstrata a definição de par ordenado. No capítulo 2 será apresentada uma definição mais "concreta".

1.9 Produto cartesiano

O *produto cartesiano* de dois conjuntos A e B, indicado por AxB, é o conjunto de os pares ordenados com primeiras componentes no conjunto A e segundas componentes no conjunto B. Por exemplo, se $A = \{a, c, d\}$ e $B = \{e, f\}$, temos:

i) Ax$B = \{(a, e), (a, f), (c, e), (c, f), (d, e), (d, f)\}$,

ii) Bx$A = \{(e, a), (e, c), (e, d), (f, a), (f, c), (f, d)\}$,

exemplos que já mostram que, de um modo geral, Ax$B \neq B$xA. (Utilizando a linguagem que será desenvolvida na seção 1.13, dizemos que o produto cartesiano não é *comutativo*).

Vamos estabelecer que um produto cartesiano do tipo AxA pode ser representado por A^2, lido "A dois". No exemplo acima temos:

i) $A^2 = \{(a, a), (a, c), (a, d), (c, a), (c, c), (c, d), (d, a), (d, c), (d, d)\}$,

ii) $B^2 = \{(e, e), (e, f), (f, f), (f, e)\}$.

1.10 Relações binárias

O conceito de produto cartesiano de dois conjuntos (iguais ou diferentes) permite que se relacione (no sentido usual do termo), dois a dois, elementos de um conjunto ou elementos de um conjunto com elementos de outro conjunto. Se A e B são dois conjuntos, um subconjunto do produto cartesiano AxB é chamado de uma *relação binária entre A e B* (ou de A em B). Ou seja, uma *relação binária entre dois conjuntos A e B* é um conjunto de pares ordenados com primeiras componentes em A e segundas componentes em B. Quando os conjuntos A e B são iguais, uma relação entre A e B é dita simplesmente uma *relação em A*. No caso de uma relação entre A e B, os elementos de A são chamados de *objetos* e um elemento de B que esteja relacionado a algum objeto é chamado *imagem* daquele objeto.

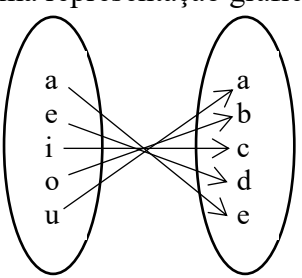
Por exemplo, se V é o conjunto das vogais e C é o conjunto das consoantes, os conjuntos $S = \{(a, b), (e, f), (i, j), (o, p), (u, v)\}$, $R = \{(a, x), (e, g), (i, b)\}$ e $T = \{(e, m), (i, z)\}$ são relações binárias entre V e C. Já o conjunto $X = \{(a, u), (e, o), (i, i),$ (o, e), (u, a)$\}$ é uma relação binária no conjunto V.

Usualmente, há interesse apenas em relações binárias em que as componentes dos pares guardem entre si alguma relação, no sentido usual do termo. Em outros termos, estamos interessados em relações

em que haja uma regra (no sentido usual do termo) para obtenção dos pares da relação, regra esta que permita que se defina se um dado par está ou não na relação. Nos exemplos acima, a relação *S* satisfaz a essa condição: cada segunda componente é a consoante que sucede a vogal primeira componente na ordem alfabética e, SMJ, as componentes dos pares das relações *R* e *T* não guardam nenhuma relação entre si e, portanto, não são relevantes. Deixamos para o leitor decidir se a relação X é ou não relevante.

Uma relação entre dois conjuntos *A* e *B* pode ser representada graficamente através dos diagramas de Venn dos dois conjuntos e de setas ligando os objetos às suas respectivas imagens.

Por exemplo, uma representação gráfica da relação X seria



Utilizando uma barra vertical significando *tal que*, pode-se representar uma relação entre dois conjuntos por $R = \{(x, y) \in A \text{x} B | \ldots\}$, onde em … é colocada a *regra* que estabelece a relação entre *x* e *y*. Por exemplo, a relação *R* do exemplo anterior poderia ser referida por $R = \{(x, y) \in V \text{x} C | y$ é a consoante sucessora de x na ordem

alfabética}. Outro exemplo, considerando os conjuntos V e C dos exemplos anteriores: se $A = \{(x, y) \in V \text{x} C | y$ é a consoante antecessora de x na ordem alfabética} temos $A = \{(e, d), (i, k), (o, n), (u, t)\}$. Observe que a vogal a não está relacionada com nenhuma consoante, pois, na ordem alfabética, não existe letra que lhe anteceda.

Observe que em $R = \{(x, y) \in A \text{x} B | \ ...\}$ o símbolo x está sendo usado para representar todos os elementos do conjunto A e y está sendo utilizado para representar todos os elementos do conjunto B. Nesse caso, dizemos que os símbolos x e y são *indeterminadas* ou *variáveis* dos conjuntos referidos.

Podemos associar um símbolo a uma relação binária em um conjunto A. Nesse caso, se o símbolo associado à relação é #, a indicação de que um par (a, b) pertence à relação é feita por $a \ \# \ b$. Dessa forma, isso pode ser utilizado para definir a relação. Por exemplo, seja A o alfabeto e consideremos a relação $\text{M} = \{(x, y) \in A^2 | \ x$ é anterior a y na ordem alfabética}. Se definirmos o símbolo $<$ para indicar essa relação, teremos $\text{M} = \{(x, y) \in A^2 | \ x < y\}$ e, então, o fato de os pares, por exemplo, (a, j) e (m, t) pertencerem à relação M pode ser indicado por $a < j$ e $m < t$.

Estudaremos mais para frente relações binárias "mais

matemáticas" e veremos que é muito útil destacar propriedades que elas satisfazem. Para facilitar a linguagem, é associada uma classificação às relações.

Dizemos que uma relação R num conjunto A é:

i) *reflexiva* se $(x, x) \in R$, qualquer que seja $x \in A$.

ii) *simétrica* se $(x, y) \in R$ implicar $(y, x) \in R$, quaisquer que sejam $x, y \in A$.

iii) *antissimétrica* se não acontece $(x, y) \in R$ e $(y, x) \in R$ com $x \neq y$, quaisquer que sejam $x, y \in A$.

iv) *transitiva* se $(x, y) \in R$ e $(y, z) \in R$ acarretar $(x, z) \in R$, quaisquer que sejam $x, y, z \in A$.

v) *total* se quaisquer que sejam $x, y \in A$, tem-se $(x, y) \in R$ e/ou $(y, x) \in R$.

(Os autores, humildemente, sugerem que o caro leitor consulte em um dicionário os significados dessas denominações na língua portuguesa).

Cada classificação é chamada também de propriedade da relação, agora com as denominações respectivas de *reflexividade*, *simetria*, *antissimetria*, *transitividade* e *totalidade*.

As definições anteriores estabelecem quando a classificação respectiva é aplicada a uma relação binária. Para facilitar a

compreensão do leitor, vamos observar as condições mínimas que negam as definições anteriores e, portanto, tal classificação não pode ser associada à relação. Com o desenvolvimento de um raciocínio simples, temos que uma relação R num conjunto A:

i) *não é reflexiva* se existe $x \in A$ tal que $(x, x) \notin R$.

ii) *não é simétrica* se existem $x, y \in A$ tais que $(x, y) \in R$ e $(y, x) \notin R$.

iii) *não é antissimétrica* se existem $x, y \in A$, com $x \neq y$, tais que $(x, y) \in R$ e $(y, x) \in R$.

iv) *não é transitiva* se existem $x, y, z \in A$ tais que $(x, y) \in R$ e $(y, z) \in R$ e $(x, z) \notin R$.

v) *não é total* se existem $x, y \in A$ tais que $(x, y) \notin R$ e $(y, x) \notin R$.

Por exemplo, se V é o conjunto das vogais, a relação $R = \{(a, a), (e, e), (i, i), (o, o), (u, u), (a, e), (a, i), (a, u), (e, a), (e, i), (e, u), (u, i)\}$ é *reflexiva*, não é *simétrica* ($(a, u) \in R$ e $(u, a) \notin R$), não é *antissimétrica* ($(a, e) \in R$, $(e, a) \in R$ e $a \neq e$), é *transitiva* e não é *total* ($(a, o) \notin R$ e $(o, a) \notin R$).

Outro exemplo: seja V o conjunto das vogais e consideremos a relação $\{(x, y) \in V \text{x} V | \text{y} = \text{x}\}$. Como cada vogal só é igual a ela mesma, os pares dessa relação são (a, a), (e, e), (i, i), (o, o) e (u, u).

Observe que as afirmações estabelecidas na seção 1.3 implicam que a *igualdade* de objetos matemáticos é *reflexiva*, *simétrica* e *transitiva*. Deixamos para o leitor determinar as propriedades que a relação X do exemplo acima satisfaz.

Para um outro exemplo, considere o *conjunto das partes* de um conjunto A definido como o conjunto de todos os subconjuntos de A e indicado por $\wp(A)$. (Infelizmente, por ora não podemos dar um exemplo de um conjunto das partes; faremos isso na seção 1.12. Como os elementos de $\wp(A)$ são conjuntos cujos elementos são elementos do conjunto A, podemos definir a relação $I = \{(X, Y) \in \wp(A) \times \wp(A) \mid X \subset Y\}$, chamada *inclusão*. As propriedades apresentadas na seção 1.5 mostram que essa relação é reflexiva, transitiva e antissimétrica. (O leitor é instado a verificar essa última afirmação!).

Uma relação que é *reflexiva*, *simétrica* e *transitiva* é dita uma *relação de equivalência* enquanto que uma relação que é *reflexiva*, *antissimétrica*, *transitiva* é dita uma *relação de ordem parcial*. Uma *relação de ordem parcial* que é *total* é dita uma *relação de ordem*. A *igualdade* de objetos matemáticos é uma *relação de equivalência*. A inclusão de conjuntos não é uma relação de equivalência (pois não é *simétrica),* mas é uma relação de ordem parcial.

Se uma relação *R,* com símbolo #, é transitiva, $x \# y$ e $y \# z$

implicam $x \# z$. Isso permite que se escreva, nesse caso, $x \# y \# z$. Por exemplo, se V é o conjunto das vogais, $X = \{a, e\}$, $Y = \{a, e, i\}$ e $Z = \{a, e, i, o\}$, temos $X \subset Y \subset Z$.

1.11 Funções

Esta seção apresentará o ente matemático pré-anunciado na seção 1.8, *função*, o conceito (na nossa opinião) mais importante da Matemática. Comecemos vendo como a língua portuguesa trata esse vocábulo, recorrendo agora ao Aulete Digital (https://www.aulete.com.br/fun%C3%A7%C3%A3o, acesso em 22/06/2020):

> função
> sf.
> **1.** Ação ou atividade própria de alguém ou de algo (função materna)
> **2.** Atividade própria de um emprego, ofício ou cargo (função de professor)
> **3.** Serventia, utilidade*: Qual a função dessa ferramenta?*
> **4.** Espetáculo, exibição, esp. de circo*: A função vai começar*
> **5.** Mat. Correspondência entre dois conjuntos, a partir de uma variável de um deles
> **6.** Exercício do entendimento, do espírito e da razão*: Está em pleno uso de suas funções intelectuais*

Observe que a acepção matemática relativa à Matemática (5.Mat Correspondência ...) não satisfaz às condições fixadas na seção

1.1 a respeito de definição de entes matemáticos (O que significa "correspondência entre dois conjuntos"? O que significa "a partir de uma variável de um deles"?).

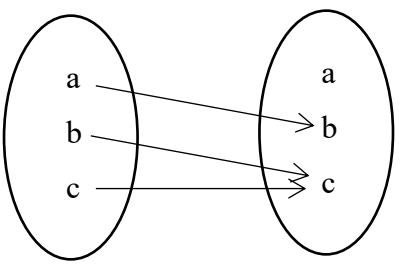
Vejamos a definição. Sejam A e B dois conjuntos. Uma *função* de A em B é uma relação binária f entre A e B tal que para cada $x \in A$ existe um único $y \in B$ tal que $(x, y) \in f$. Assim, para que uma relação binária f entre dois conjuntos A e B seja uma função de A em B, para todo $x \in A$ tem que existir $y \in B$ tal que $(x, y) \in f$ e que se $(x, y_1) \in f$ e $(x, y_2) \in f$ então $y_1 = y_2$. Ou seja, tem que existir tal y e ele deve ser único.

Por exemplo, se V é o conjunto das vogais e C é o conjunto das consoantes, a relação entre V e C $f = \{(a, b), (e, f), (i, j), (o, p), (u, v)\}$ é uma função de V em C. Por seu turno, é fácil ver que a relação X da seção anterior é uma função de V em V. Já a relação R = $\{(a, e), (a, i), (a, o), (a, u), (e, i), (e, o), (e, u), (i, o), (i, u), (o, u)\}$ não é uma função de V em V, pois a vogal a tem mais de uma imagem (isso já bastaria para a relação não ser uma função) e, adicionalmente, o objeto u não tem imagem. Também a relação $I = \{(X, Y) \in \wp(A) \times \wp(A) \mid X \subset Y\}$, com $A = \{a, b, c\}$, não é uma função de $\wp(A)$ em $\wp(A)$ pois $(\{a\}, \{a, b\}) \in I$ e $(\{a\}, \{a, c\}) \in I$.

Como já vimos fazendo, utilizaremos letras minúsculas f, g, h etc. para representar funções e escreveremos $y = f(x)$, para indicar que

$(x, y) \in f$ (no futuro, usaremos também cadeia de caracteres para indicar funções). Como em relações binárias, diremos que $y = f(x)$ é a *imagem* do *objeto* x pela função f (dizemos também que f *mapeia* x *em* y ou que f *leva* x *em* y). Com isso, a definição de função pode ser escrita da seguinte forma: uma *função* de A em B é uma relação binária f entre A e B tal que cada objeto tem uma única imagem.

Também como em relações, poderemos representar graficamente uma função pelos diagramas de Venn. Por exemplo, se $A = \{a, b, c\}$, a função f de A em A, dada por $f = \{(a, b), (b, c), (c, c)\}$ pode ser representada por



Se f é uma função de um conjunto A em um conjunto B, o conjunto A é chamado *domínio*, indicado por $D(f)$, e o conjunto B é chamado *contradomínio* de f. O subconjunto do contradomínio cujos elementos são imagens de objetos é chamado *imagem da função*, indicada por $f(A)$. No exemplo, $D(f) = \{a, b, c\}$ e

$f(A) = \{b, c\}$

Uma função f de A em B dada por $y = f(x)$ pode ser representada por

$$f : A \rightarrow B$$
$$x \rightarrow f(x).$$

Nesse caso, $y = f(\text{x})$ fixa a regra que será utilizada para se associar um único $y \in B$ a cada $x \in A$.

Nada impede que a regra que associa uma única imagem a cada objeto seja constituída de várias *sub-regras* de acordo com valores dos objetos. Por exemplo, se A é o alfabeto podemos definir a função g de A em A por:

$$g : A \rightarrow A$$
$$x \rightarrow g(x) = \begin{cases} a, \text{se } x = z \\ \text{letra sucessora de } x, \text{se } x \neq \text{z}. \end{cases}$$

Num caso como esse, pode-se utilizar expressões como *caso contrário*, *senão*, *em outra hipótese* para indicar as situações em que a última *sub-regra* será aplicada.

É importante verificar se uma pretensa definição define realmente uma função, caso em que se diz que a função está *bem definida*. Naturalmente, para que uma função f esteja *bem definida* é necessário que para todos os objetos k e j existam $f(k)$ e $f(j)$ e se $f(k) \neq f(j)$, se tenha $k \neq j$.

Como foi dito anteriormente, ao se estudar um novo objeto matemático devemos estabelecer quando dois desses objetos serão considerados iguais. Para funções temos a seguinte definição. Duas funções f e g são iguais quando possuem os mesmos domínio e contradomínio e para todo objeto x do domínio se tem $f(x) = g(x)$. Isto significa que duas funções iguais são, na verdade, a mesma (no sentido usual do termo) função.

Dois exemplos de funções que serão utilizadas em exemplos futuros e em demonstrações são apresentados a seguir.

1. Seja A um conjunto. A função de A em A definida por $I(x) = x$ é chamada função *identidade* do conjunto A e é simbolizada por I_A.

2. Sejam A e B dois conjuntos, f uma função de A em B e C um subconjunto de A. A função $g : C \to B$ definida por $g(x) = f(x)$ é chamada de *restrição* de f ao subconjunto C e é indicada por $f/_C$. Por exemplo, se A é o alfabeto e V é o conjunto das vogais, a função h de V em A tal $h(x)$ é a letra sucessora de x na ordem alfabética é a restrição da função g do exemplo anterior ao conjunto das vogais: $h = g/_V$.

1.12 Predicados em um conjunto e o conjunto vazio

Vimos acima que um conjunto pode ser representado pela exibição de seus elementos entre chaves ou no interior de uma curva fechada. O conceito de função e a utilização da barra vertical significando *tal que* permite uma outra forma de representar um conjunto. Esta nova forma de representar conjuntos permitirá a definição de um conjunto muito especial. Para tal, necessitamos de alguns novos conceitos.

O conjunto $B = \{V, F\}$ (V significando *verdadeiro* e F, *falso*) é chamado *conjunto de Boole*. Um *predicado* ou uma *sentença aberta* em um conjunto A é uma função de A no conjunto de Boole. Nesse caso, a imagem de um objeto é chamada *valor lógico*. Por exemplo, se A é o conjunto das letras do alfabeto, podemos definir um predicado em A por $p(x) = V$, se x é uma vogal e $p(x) = F$, se x é uma consoante. Nesse exemplo, temos $p(a) = V$ e $p(b) = F$. Como as imagens dos objetos podem ser apenas V ou F, vamos definir predicados indicando apenas quando a imagem do objeto será V. O predicado do exemplo anterior será definido apenas por $p(x) = V$ se x é vogal.

Vale a pena observar que na definição do predicado, o símbolo x não está representando especificamente a letra x e sim uma

indeterminada do conjunto. No exemplo anterior, para a letra x, temos $p(x) = F$. Observe que, em outros termos, um predicado num conjunto A é uma propriedade que é verdadeira para alguns elementos de A e falsa para outros. Além disso, para todo elemento do conjunto A a tal propriedade é verdadeira ou falsa (apenas uma das condições), não havendo uma terceira possibilidade. Essa observação permite que um predicado seja definido explicitando apenas a tal propriedade a qual ele se refere. Assim, o predicado *p(x) = V se x é uma vogal* pode ser referido apenas por *x é uma vogal*.

Uma outra forma de representar um conjunto é a seguinte. Se A é um conjunto e p é um predicado em A, $\{x \in A | \ p\}$ representa o subconjunto dos elementos de A para os quais $p(x) = V$. Por exemplo, se A é o conjunto das letras do alfabeto, o conjunto das vogais pode ser representado por $B = \{x \in A | \ x$ é uma vogal$\}$.

Um predicado p num conjunto A é uma *contradição* se $p(x) = F$ para todo elemento $x \in A$ e é uma *tautologia* se $p(x) = V$ qualquer que seja $x \in A$. Por exemplo, se A é um conjunto qualquer, o predicado em A dado por $x \neq x$ é uma *contradição* e o predicado em A dado por $x \in A$ é uma *tautologia*. Uma *contradição* e uma *tautologia* serão representadas por γ e τ, respectivamente.

O conceito de contradição permite a definição de um conjunto, aparentemente estranho, mas de importância fundamental para a

Matemática. Se A é um conjunto qualquer e γ é uma contradição em A o conjunto $\{x \in A|\gamma\}$ não possui elementos, é chamado *conjunto vazio* e é representado pelo símbolo $\varnothing$. Por exemplo, se A é o alfabeto, o conjunto $\{x \in A|\ x \neq x\}$ é o conjunto vazio. Um conjunto diferente do conjunto vazio é dito *não vazio*.

Na seção 1.15 provaremos que o conjunto vazio é subconjunto de qualquer conjunto: $\varnothing \subset A$, qualquer que seja o conjunto A. Considerando esse fato, podemos agora dar um exemplo de um conjunto das partes de um conjunto, conceito introduzido na seção 1.10: se $A = \{a, b, c\}$, $\wp(A) = \{\varnothing, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$.

1.13 Operações

No nosso caminhar ao longo da trilha da Matemática, desde a nossa tenra idade deparamo-nos com o aprender a realizar *operações*: somar, subtrair, multiplicar etc. Nesta seção, o conceito de operações será formalizado. Inicialmente, observemos como os dicionários tratam o significado de operação (https://www.aulete.com.br/opera%C3%A7%C3%A3o, acesso em 23/06/2020):

operação
sf.
1. Ação ou resultado de operar.
2. Ação altamente organizada, envolvendo muitas pessoas incumbidas de diferentes tarefas: operação de resgate das vítimas.
3. Ação ou conjunto de ações visando alcançar determinado resultado: operação de trânsito.
4. Ação ou resultado de fazer funcionar; FUNCIONAMENTO: Entrou em operação novo provedor de internet grátis.
5. Econ. Compra ou venda de valores ou mercadorias; transação comercial (operações cambiais).
6. Mat. Cálculo matemático: operação de adição.
7. Med. Cirurgia (operação cardíaca).
8. Mil. Ação ou manobra militar.
9. Quím. Série de preparações que têm por fim a dissociação, a combinação ou a simples mistura dos diversos elementos.

Mais uma vez, observa-se que as concepções dicionaristas não contemplam as condições mínimas para uma definição matemática (na acepção 6, o que é "cálculo matemático"? O que é "operação de adição"?). Ou seja, precisamos de uma definição de acordo com as exigências da Linguagem Matemática como a que segue (pedimos ao leitor que observe sua simplicidade!):

Uma *operação* num conjunto A é uma função de AxA em A, ou seja, uma operação associa a um par de elementos de um conjunto um elemento do conjunto. Por exemplo, no conjunto das vogais V podemos definir a operação f dada por $f(a, a) = e$,

$f(a, e) = i, f(a, i) = o$, ..., e observa-se que seria enfadonho escrevermos as imagens de todos os objetos. Uma forma mais cômoda e sensata é apresentar a operação através de uma tabela, na qual o elemento da linha i e da coluna j apresenta a imagem do par (i, j).

	a	e	i	o	u
a	e	i	o	u	a
e	i	o	u	a	e
i	o	u	a	e	i
o	u	a	e	i	o
u	a	e	i	o	u

Um outro exemplo: no conjunto dos dias da semana S = {Dom, Seg, Ter, Qua, Qui, Sex, Sab} podemos definir a operação dada pela tabela a seguir.

	Dom	Seg	Ter	Qua	Qui	Sex	Sab
Dom	Seg	Ter	Qua	Qui	Sex	Sab	Dom
Seg	Ter	Qua	Qui	Sex	Sab	Dom	Seg
Ter	Qua	Qui	Sex	Sab	Dom	Seg	Ter
Qua	Qui	Sex	Sab	Dom	Seg	Ter	Qua
Qui	Sex	Sab	Dom	Seg	Ter	Qua	Qui
Sex	Sab	Dom	Seg	Ter	Qua	Qui	Sex
Sab	Dom	Seg	Ter	Qua	Qui	Sex	Sab

Os autores, humildemente, concordam com o leitor que esses exemplos não são muito esclarecedores. Porém, eles, com algumas adaptações, serão úteis no entendimento do que será estudado no capítulo 3. Além disso, nas seções seguintes teremos exemplos mais

consistentes de operação. Nesses exemplos, fixaremos símbolos específicos para operação e, ao invés de utilizarmos a notação usual de função $f(x, y)$, usaremos $x \# y$ quando o símbolo da operação é #. O símbolo associado à operação é chamado *operador*, as componentes do par objeto (a, b) são chamados de *operandos* e a imagem $a \# b$ é o *resultado* e receberá uma denominação específica para cada operação. (Quando a operação for dada por uma tabela, vamos explicitar o operador na primeira célula). Por exemplo, se escolhermos o operador **+** (lido *mais*) para a operação no conjunto dos dias da semana, temos Qui + Sex = Qua, Seg + Sex = Dom etc. O interessante é que, como mostraremos no capítulo 3, há uma lógica (no sentido usual do termo) para essa operação.

Naturalmente, podem ser realizadas aplicações sucessivas de uma operação. Nesse caso, usa-se parênteses para indicar quais resultados "parciais" devem ser obtidos. Utilizando o operador **+** para a operação do exemplo do conjunto das vogais e chamando o resultado da operação de *soma*, $(a + e) + o$ indica que se deve determinar a soma de a com e e, em seguida, determinar a soma desta soma com o. Assim, temos $(a + e) + o = i + o = e$. Uma representação de aplicações sucessivas de uma ou mais operações é chamada de *expressão*.

Observe que nos dois exemplos a ordem dos operandos não

altera o resultado. Observe também que o resultado da operação de qualquer vogal com *u* é a própria vogal, o que também acontece com operações com Sab no segundo exemplo. Como as relações binárias, as operações também podem ser classificadas de acordo com propriedades que ela satisfizer.

Seja A um conjunto e # uma operação em A. Dizemos que a operação #

i) é *comutativa* se $a \# b = b \# a$, quaisquer que sejam a, $b \in A$.

ii) é *associativa* se $a \# (b \# c) = (a \# b) \# c$, quaisquer que sejam a, b, $c \in A$.

iii) possui um *elemento neutro e* se existe um elemento $e \in A$ tal que $a \# e = e \# a = a$, qualquer que seja $a \in A$.

Os comentários feitos no início do período anterior mostram que as duas operações exemplificadas são comutativas e possuem elementos neutros (*u* da primeira e Sab da segunda). É fácil (mas muito extenuante) ver que as duas operações são associativas. Por exemplo, $a + (e + o) = a +$ a $= e$ e $(a + e) + o = i + o = e$, ou seja, $a + (e + o) = (a + e) + o$. A questão é que um mero caso não comprova a afirmação. Para isso, teríamos de verificar as igualdades respectivas para todos os ternos (no sentido usual do termo) de vogais.

Quando a operação está denotada na forma de função,

$f(a, b)$, forma de representação chamada *notação prefixa*, as classificações acima são referenciadas da seguinte forma.

Uma operação f definida num conjunto A

i) é *comutativa* se $f(a, b) = f(b, a)$, quaisquer que sejam $a, b \in A$.

ii) é *associativa* se $f(a, f(b, c)) = f(f(a, b), c)$, quaisquer que sejam $a, b, c \in A$.

iii) possui um *elemento neutro* e se existe um elemento $e \in A$ tal que $f(a, e) = f(e, a) = a$, qualquer que seja $a \in A$.

A referência a cada uma destas propriedades é feita, de maneira óbvia, como *comutatividade*, *associatividade*, *existência de elemento neutro*.

Observe que se uma operação o possuir, o elemento neutro é único. De fato, se e' e e'' são elementos neutros de uma operação #, temos, por um lado, $e' \# e'' = e'' \# e' = e'$, pois e'' é elemento neutro e, por outro, $e'' \# e' = e' \# e'' = e''$, pois e' é elemento neutro. Assim, pela transitividade da igualdade, $e' = e''$.

Vamos estabelecer que em uma operação associativa não há a necessidade da colocação de parênteses. Se # é o operador de uma operação associativa, como $a \# (b \# c) = (a \# b) \# c$, vamos indicar a

$\#\,(b\,\#\,c)$ por $a\,\#\,b\,\#\,c$, como se estivéssemos operando três operandos. Essa flexibilização da notação se estende também quando há "mais de três operandos". Quando há mais de dois operandos (e a operação é associativa, lembremo-nos), o mais prático é determinar o resultado da operação dos dois primeiros, operar este resultado com o próximo operando e, assim, sucessivamente. No exemplo das vogais, por exemplo, temos

$$e + o + a + i = a + a + i = e + i = u.$$

Além da comutatividade, associatividade e existência de elemento neutro, uma operação pode ser classificada em relação à outra operação. Se # e * são operações definidas num conjunto A, dizemos que # é *distributiva em relação à* * se $a\,\#\,(b * c) = (a\,\#\,b) * (a\,\#\,c)$, quaisquer que sejam $a, b, c \in A$. Essa propriedade é referida como *distributividade* da operação # em relação à operação *.

Na notação prefixa, a distributividade seria assim fixada: sejam f e g duas operações num conjunto A. A operação f é distributiva em relação à operação g se $f(a, g(b, c)) = g(f(a, b), f(a, c))$, quaisquer que sejam $a, b, c \in A$.

À medida que formos apresentando as operações, discutiremos quais propriedades elas possuem e apresentaremos exemplos dessas propriedades.

1.14 Operações com predicados (operações lógicas)

As primeiras operações que discutiremos são as operações onde os operandos são predicados. Como veremos, as operações com predicados (também chamadas *operações lógicas*) estabelecem termos que enriquecem sobremaneira a linguagem matemática.

Dado um conjunto não vazio A, representemos por $Pred(A)$ o conjunto dos predicados em A, ou seja (para lembrar), $Pred(A)$ é o conjunto de todas as funções de A no conjunto de Boole $B = \{V, F\}$.

Pelo conceito de operação, para se definir uma operação em $Pred(A)$ devemos associar a cada par de predicados de $Pred(A)$ um outro predicado de $Pred(A)$. Como já foi dito, para se definir um elemento de $Pred(A)$, basta se estabelecer as imagens dos elementos de A em $\{V, F\}$. Temos as seguintes operações, considerando $p, q \in Pred(A)$.

i) *Conjunção* (operador: $\wedge$, denominação: **e**)

$$(p \wedge q)(x) = \text{V se } p(x) = q(x) = \text{V}.$$

Isto é, a *conjunção* de dois predicados p e q será verdadeira quando e somente quando os dois predicados o forem. Daí a

denominação **e** para o operador $\wedge$, indo ao encontro da língua portuguesa: se alguém anuncia "nas férias, viajaremos para Maceió **e** Natal", ele está afirmando que a família viajará para as duas cidades.

Como a igualdade é uma relação simétrica (por exemplo, se $p(x) = q(x) = V$ então $q(x) = p(x) = V$), a conjunção é comutativa. Ela também é associativa: se p, q e r são predicados em A, por um lado $((p \wedge q) \wedge r)(x) = V$ se $(p \wedge q)(x) = r(x) = V$, o que só acontece se $p(x) = q(x) = r(x) = V$ e por outro lado $(p \wedge (q \wedge r))(x) = V$ se $p(x) = (q \wedge r)(x) = V$ o que só acontece também se $p(x) = q(x) = r(x) = V$. Claramente, uma tautologia τ é o elemento neutro da conjunção.

ii) *Disjunção* (operador: $\vee$, denominação: **ou**)

$(p \vee q)(x) = \mathrm{F}$ se $p(x) = q(x) = \mathrm{F}$.

Isto é, o valor lógico de uma *disjunção* de dois predicados p e q somente é falso se os valores lógicos de p e de q são falso, ou seja, para que a conjunção de p e q seja verdadeira basta que o valor lógico de um dos predicados seja verdadeiro ou que os valores lógicos de ambos predicados sejam verdadeiro. Observe agora que a denominação **ou** para o operador $\vee$ não corresponde exatamente ao uso da conjunção **ou** na linguagem comum: se alguém anuncia "nas férias viajaremos para Maceió **ou** Natal", ele está afirmando que a

família viajará para apenas uma das duas cidades. Dizemos que o **ou** da Matemática é *inclusivo*, enquanto o **ou** da língua portuguesa é *exclusivo*. Embora nem todo dicionário apresente esta possibilidade, algumas gramáticas adotam o uso de **e/ou** na linguagem comum quando se pretende se expressar um "ou inclusivo". Daqui para frente, a conjunção **ou** utilizada em afirmações matemáticas terá sempre o sentido inclusivo. Dessa forma, o conceito de totalidade de uma relação, discutido na seção 1.9, pode ser escrito: uma relação binária num conjunto A é *total* se quaisquer que sejam $x, y \in A$, com $x \neq y$, $(x, y) \in R$ ou $(y, x) \in R$.

Como a conjunção, a disjunção é comutativa e associativa e seu elemento neutro é uma contradição γ.

O exercício 1.5 pedirá para ser demonstrado que a conjunção é distributiva em relação à disjunção e que esta é distributiva em relação àquela.

iii) *Implicação* (operador $\Rightarrow$, denominação: **implica**)

$(p \Rightarrow q)(x) = \text{F}$ se $p(x) = \text{V}$ e $q(x) = \text{F}$.

O predicado $p \Rightarrow q$ também pode ser lido *se p, então q* e quando p e q são verdadeiros tem a conotação da linguagem comum: "se não chover, então vamos para praia" (quase sempre com o advérbio *então* elipsado e guardando uma relação de causa e efeito). Observe que, diferentemente da linguagem comum, $p \Rightarrow q$ somente é

falso se p é verdadeiro e q é falso. Ou seja, na linguagem matemática uma "mentira" implica uma "verdade" e implica também outra "mentira".

O exemplo a seguir mostra que o significado matemático do *se*, *então*, embora inusitado, tem sentido também no nosso dia a dia. Imagine a seguinte situação: (1) uma jovem adolescente está se preparando, com afinco, para fazer o vestibular para um curso superior; (2) para incentivá-la na reta final, o pai, a dois meses do certame, adquire um automóvel e anuncia para ela: *se você for aprovada, este automóvel será seu*.

Após a divulgação do resultado do vestibular, se a filha foi aprovada (p verdade) e recebeu o carro (q verdade), a afirmação do pai se tornou verdadeira ($p \Rightarrow q$ verdade); se a filha foi aprovada (p verdade) e não recebeu o carro (q falso), a afirmação do pai se tornou falsa ($p \Rightarrow q$ falso); se a filha não foi aprovada (p falso) e não recebeu o carro (q falso), o pai não descumpriu a promessa ($p \Rightarrow q$ verdade); finalmente, se a filha não foi aprovada (p falso) e recebeu o carro (q verdade), a afirmação do pai também não se tornou falsa e, portanto $p \Rightarrow q$ é verdadeiro (nesse caso, o pai pode ter entendido que a filha, mesmo não tendo sido aprovada, merecia o prêmio – foi a primeira dos não aprovados, por exemplo).

Como $p \Rightarrow q$ só é falso se p é verdadeiro e q é falso, a

demonstração de uma assertiva do tipo "se *p,* então *q*" pode ser feita supondo-se que *p* é verdade e provando que, a partir daí, *q* também o é. Em um caso como esse, o predicado *p* é chamado *hipótese* (que é o que se supõe ser verdadeiro) e o predicado *q* é chamado *tese* (que é o que se quer provar que é verdadeiro). Por exemplo, na seção 1.5 provamos que "se $A \subset B$ e $B \subset C$, então $A \subset C$, quaisquer que sejam os conjuntos A, B e C". Nesse caso, a hipótese é "$A \subset B$ e $B \subset C$" e a tese, "$A \subset C$". Usando os recursos da linguagem matemática que já dispomos, essa propriedade poderia ser escrita da seguinte forma: $(A \subset B \wedge B \subset C) \Rightarrow A \subset C$, quaisquer que sejam os conjuntos A, B e C. (Ainda veremos mais uma "ação simplificadora" da linguagem matemática a essa propriedade).

iv) *Equivalência* (operador $\Leftrightarrow$, denominação: **equivale**)

$$(p \Leftrightarrow q)(x) = \text{V se } p(x) = q(x).$$

O predicado $p \Leftrightarrow q$ também é referenciado como *p se e somente se q* e, SMJ, não há expressão equivalente (agora, no sentido usual do termo) na língua portuguesa. É fácil ver que uma equivalência pode ser obtida a partir de uma conjunção de implicações: $p \Leftrightarrow q = (p \Rightarrow q) \wedge (q \Rightarrow p)$.

A demonstração de uma igualdade de predicados é bastante simples (embora, às vezes, tediosa). Como são funções, para que dois

predicados r e s sejam iguais, basta que eles tenham o mesmo domínio (no nosso caso, conjunto A), o mesmo contradomínio (sempre $B = \{V, F\}$) e para cada x de A se tenha $r(x) = s(x)$. Basta então mostrar a igualdade $r(x) = s(x)$, para todo $x \in A$, o que pode ser feito através de uma tabela (chamada *tabela verdade*) na qual se determina todos os possíveis valores de $r(x)$ e $s(x)$. Para mostrar que $r = p \Leftrightarrow q$ e $s = (p \Rightarrow q) \wedge (q \Rightarrow p)$ são iguais, temos

p	q	$p \Rightarrow q$	$q \Rightarrow p$	$p \Leftrightarrow q$	$(p \Rightarrow q) \wedge (q \Rightarrow p)$
V	V	V	V	V	V
V	F	F	V	F	F
F	V	V	F	F	F
F	F	V	V	V	V

Da igualdade $p \Leftrightarrow q = (p \Rightarrow q) \wedge (q \Rightarrow p)$, segue que uma afirmação do tipo q se e somente se p pode ser demonstrada supondo que p é verdade e provando que, a partir daí, q também é e, reciprocamente, supondo que q é verdade e provando que, a partir daí, p também é.

Tabelas verdade também podem ser utilizadas para definir as operações lógicas:

p	q	$p \wedge q$	$p \vee q$	$p \Rightarrow q$	$p \Leftrightarrow q$
V	V	V	V	V	V
V	F	F	V	F	F
F	V	F	V	V	F
F	F	F	F	V	V

Além das quatro operações lógicas, que, por definição de operação, associam a dois predicados um outro, há uma "quinta operação" (dita uma *operação unária*), que "atua" em um único predicado, chamada *negação*, com operador ~, chamado **não**, definida por: $(\sim p)(x) = \text{F}$ se $p(x) = \text{V}$ (ou $\sim p(x) = \text{F}$ se $p(x) = \text{V}$).

Tem mais. O leitor deve ter observado que as expressões "qualquer que seja", "existe um" e seus plurais aprecem em diversas definições e propriedades. A linguagem matemática dispõe de símbolos para substituir essas expressões: o *quantificador universal*, $\forall$, "qualquer que seja", "para todo" e seus plurais, e o *quantificador existencial*, $\exists$, "existe um" e seus plurais. Por exemplo, a propriedade apresentada na seção 1.5 provamos que "se $A \subset B$ e $B \subset C$, então $A \subset C$, quaisquer que sejam os conjuntos A, B e C" poderia ser escrita na forma "$(A \subset B \wedge B \subset C) \Rightarrow A \subset C$, $\forall A$, B e C".

1.15 Demonstração por redução ao absurdo (prova por contradição)

Como foi dito na seção anterior, a demonstração de uma assertiva matemática do tipo "se *p,* então *q*" pode ser feita supondo-se que *p* é verdade e provando que, a partir daí, *q* também o é. Nesta seção, apresentaremos duas outras maneiras de se demonstrar afirmações da forma "se *p,* então *q*", ambas chamadas *demonstração por redução ao absurdo* ou *prova por contradição*. Para isso, observe que a tabela verdade

p	q	$p \Rightarrow q$	$\sim q$	$\sim p$	$(\sim q) \Rightarrow (\sim p)$
V	V	V	F	F	V
V	F	F.	V	F	F
F	V	V	F	V	V
F	F	V	V	V	V

que mostra $(p \Rightarrow q) = ((\sim q) \Rightarrow (\sim p))$. Assim, outra forma de se provar uma afirmação matemática do tipo "se *p,* então *q*" é supor que *q* é falso e concluir, a partir daí, que *p* também o é. Ou seja, para provar que "uma hipótese implica uma tese" pode-se demonstrar que a negação da tese implica a negação da hipótese. (Como a hipótese é suposta verdadeira, ela não pode ser negada, o que aconteceria se a tese fosse negada. Logo a tese é verdadeira).

Por exemplo, para demonstrar que o conjunto vazio é subconjunto de qualquer conjunto, como dito na seção 1.12, suponhamos que exista um conjunto A tal que $\varnothing \not\subset A$ (negação da tese). Daí, teríamos a existência de um elemento do conjunto $\varnothing$ que não pertence ao conjunto A. Porém, a existência de um elemento de $\varnothing$ negaria a hipótese ($\varnothing$ é vazio).

Também é fácil provar (ver exercício 1.9) que $(p \Rightarrow q) = ((p \wedge (\sim q)) \Rightarrow \gamma)$, onde p e q são predicados em um conjunto A e γ é uma contradição. Assim, também se pode provar uma afirmação da forma "se p, então q", provando-se que a veracidade da hipótese e a negação da tese implicam uma contradição. Isto demonstra que a veracidade da hipótese implica a veracidade da tese. Veremos vários exemplos de demonstração por redução ao absurdo ao longo do livro. Nestes exemplos, quase sempre, utilizaremos as expressões "suponhamos, por contradição, que" ou "por redução, suponhamos que" quando vamos negar a tese.

1.16 Operações com conjuntos

Seja U um conjunto e consideremos $\wp(U)$ o conjunto das partes de U. Quando se está trabalhando com conjuntos que são

subconjuntos de um conjunto U, este conjunto U é chamado *conjunto universo*. Até agora, e continuaremos ainda neste capítulo, o nosso universo tem sido o alfabeto.

Pelo seu conceito, para se definir uma operação em $\wp(U)$ devemos associar a cada par de subconjuntos de U um outro subconjunto deste conjunto. Temos as seguintes operações, considerando $A, B \subset U$:

i) *União* (operador: $\cup$, denominação: **união**)

$$A \cup B = \{x \in U | (x \in A) \vee (x \in B)\}$$

Pela definição da operação lógica disjunção, a união de dois conjuntos é o conjunto dos elementos que pertencem a pelo menos um dos conjuntos.

ii) *Interseção* (operador: $\cap$; denominação: **interseção**)

$$A \cap B = \{x \in U | (x \in A) \wedge (x \in B)\}$$

Pela definição da operação lógica conjunção, a interseção de dois conjuntos é o conjunto dos elementos que pertencem aos dois conjuntos.

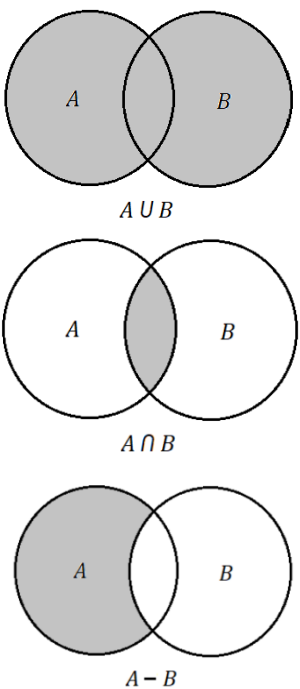
iii) *Diferença* (operador: **-**; denominação: **menos**)

$$A - B = \{x \in U | (x \in A) \wedge (x \notin B)\}$$

Aplicando novamente a definição de conjunção, temos que a diferença entre dois conjuntos A e B é o conjunto dos elementos que

pertencem exclusivamente ao conjunto A (ou os elementos que pertencem a A e não pertencem a B).

Utilizando os diagramas de Venn, essas operações seriam representadas graficamente por (fonte: https://www.infoescola.com/matematica/teoria-dos-conjuntos/, acesso em: 26/06/2020)



Para um exemplo, se A = {a, c, e, f} e B {c, d , f, g}, $A \cup B$ = {a, c, d, e, f, g}, $A \cap B$ = {c, f}, A - B = {a, e} e B - A = {d, g}.

Como consequência da comutatividade e da associatividade da conjunção e da disjunção, a união e a interseção de conjuntos são comutativas e associativas. O exemplo acima mostra que a diferença entre conjuntos não é comutativa (um exemplo de um ente matemático que mostra que uma operação e uma relação não satisfazem uma determinada propriedade é chamado de *contraexemplo*). Deixamos para o leitor obter um contraexemplo que mostra que a diferença não é associativa.

Como o conjunto vazio $\varnothing$ não tem elementos temos que $A \cup \varnothing = A$, qualquer que seja o subconjunto A, e, portanto, $\varnothing$ é o elemento neutro da união (observe que não há necessidade de fazer referência a $\varnothing \cup A = A$, pois a união é comutativa). Observe também que mesmo sendo verdade que $A - \varnothing = A$, o conjunto vazio não é elemento neutro da diferença, pois, se $A \neq \varnothing$, $\varnothing - A \neq A$. De fato, a diferença não tem elemento neutro. Devido ao fato de que $A \cap U = A$, qualquer que seja o subconjunto de U, o universo U é o elemento neutro da interseção.

1.17 Uma operação com funções

Seja A um conjunto e indiquemos por $\mathfrak{I}(A)$ o conjunto das funções de A em A. Em $\mathfrak{I}(A)$ definimos a operação *composição de funções* associando a cada par de funções $(f, g) \in \mathfrak{I}(A)$ a *função composta de f e g*, representada por $f \circ g$, definida por $(f \circ g)(x) = f(g(x))$.

Por exemplo, se A é o conjunto das vogais, $f = \{(a, e), (e, i), (i, o), (o, u), (u, a)\}$ e g = $\{(a, i), (e, i), (i, o), (o, o), (u, a)\}$ temos $f \circ g = \{(a, o), (e, o), (i, u), (o, u), (u, e)\}$ pois

$$(f \circ g)(\text{a}) = f(g(a)) = f(i) = o;$$

$$(f \circ g)(e) = f(g(e)) = f(i) = o;$$

$$(f \circ g)(i) = f(g(i)) = f(o) = u;$$

$$(f \circ g)(o) = f(g(o)) = f(o) = u;$$

$$(f \circ g)(u) = f(g(u)) = f(a) = e.$$

Por outro lado, $g \circ f = \{(a, i), (e, o), (i, o), (o, a), (u, i)\}$ pois

$$(g \circ f)(a) = g(f(a)) = g(e) = i;$$

$$(g \circ f)(e) = g(f(e)) = g(i) = o;$$

$$(g \circ f)(i) = g(f(i)) = g(o) = o;$$

$$(g \circ f)(o) = g(f(o)) = g(u) = a;$$

$$(g \circ f)(u) = g(f(u)) = g(a) = i.$$

Claramente, para todo $x \in A$, $(f \circ I_A)(x) = f(I_A(x)) = f(x)$ e $(I_A \circ f)(x) = I_A(f(x)) = f(x)$, igualdades que mostram que $I_A \circ f = f \circ I_A = f$. Isso prova que a função identidade (definida na seção 1.11) é o elemento neutro da composição de funções.

Observe que, se $f, g, h \in \mathfrak{I}(A)$,

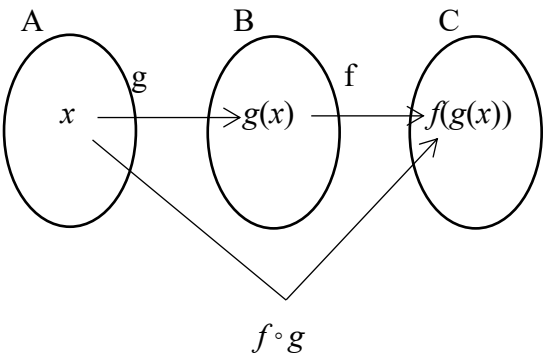
$$(f \circ (g \circ h))(x) = f((g \circ h)(x)) = f(g(h(x))),$$

$$((f \circ g) \circ h)(x) = (f \circ g)(h(x)) = f(g(h(x))),$$

o que mostra que a composição de funções é associativa. Observe também que o exemplo anterior mostra que a composição de funções não é comutativa.

Se A e B são dois conjuntos representa-se por $\mathfrak{I}(A, B)$ o conjunto das funções de A em B. Se C é um terceiro conjunto, a operação composição de funções pode ser "generalizada" para se associar a um par de funções $(g, f) \in \mathfrak{I}(A, B) \times \mathfrak{I}(B, C)$ uma função de $\mathfrak{I}(A, C)$.

Se g é uma função de A em B e f é uma função de B em C, a *composta* das funções f e g é a função $f \circ g$ de A em C definida por $(f \circ g)(x) = f(g(x))$. Em termos de diagrama de Vem, teríamos a seguinte representação gráfica, que evidencia que um elemento de A é levado diretamente na sua imagem em C pela função composta $f \circ g$, "sem passar" pelo conjunto B.



Observe que essa definição não atende plenamente o conceito de operação em um conjunto dada na seção 1.13, o que justifica as aspas utilizadas na palavra generalizada acima. De fato, f e g são elementos de dois conjuntos distintos e $f \circ g$ é elemento de um terceiro conjunto.

Observe também que se A, B, C e D são conjuntos e f, g e h são funções dos conjuntos $\mathfrak{I}(A, B)$, $\mathfrak{I}(B, C)$ e $\mathfrak{I}(C, D)$, respectivamente, temos $(f \circ g) \circ h = f \circ (g \circ h)$, o que pode ser provado da mesma forma que se provou a associatividade da composição de funções.

1.18 Funções inversíveis

O primeiro exemplo da seção 1,13 apresentou uma operação que possuía o elemento neutro u. Se voltarmos a esse exemplo,

poderemos observar que dado qualquer elemento $x \in V$, existe um elemento $y \in V$ tal que $x + y = u$ (por exemplo, $e + i = u$). Esse fato não ocorre a união de conjuntos estudada na seção 1.15. Embora a união tenha elemento neutro, $\varnothing$, dado um subconjunto não vazio X, não existe um subconjunto Y tal que $X \cup Y = \varnothing$. A existência de um elemento que "neutraliza" um elemento em relação a uma operação é contemplada com uma denominação específica, o que enriquece ainda mais a linguagem matemática. Seja # uma operação em um conjunto A que possui um elemento neutro e. Dizemos que um elemento x de A *tem simétrico* se existe um elemento $y \in A$ tal que $x \# y = y \# x = e$.

É interessante observar que se a operação # for associativa e um elemento x tiver simétrico, então esse simétrico é único e poderemos falar em o simétrico de x. Para provar esse fato, suponhamos que a operação # é associativa e que y' e y'' sejam simétricos de x (aqui será mostrada uma técnica muito utilizada para se provar que algo é único: supõe-se que existem dois, e prova-se que eles são iguais). Temos a seguinte sequência de implicações, justificadas ao lado:

$y' = y' \#$ e (e é elemento neutro)

$y' = y' \# (x \# y'')$ (y'' é simétrico de x e, portanto, $x \# y'' = e$)

$y' = (y' \# x) \# y''$ (# é associativa)

$y' = e \# y$" (y' é simétrico de x, e, portanto, $y' \# x = e$)

$y' = y$" (e é elemento neutro)

A unicidade de simétrico de um elemento x em relação a uma operação associativa permite que fixemos uma denominação para ele. Em algumas operações, o simétrico do elemento x continua sendo chamado *simétrico de x* e é representado por -x. Em outras operações, o simétrico é dito *inverso de x*, caso em que é representado por x^{-1}.

Como vimos na seção anterior, a composição de funções definida em $\mathfrak{I}(A)$ tem elemento neutro I_A. Vamos discutir em que condições uma função f de $\mathfrak{I}(A)$ possui simétrico em relação à composição. Ou seja, vamos discutir as condições em que dada uma função f de $\mathfrak{I}(A)$ existe uma função g de $\mathfrak{I}(A)$ tal que $f \circ g = g \circ f = I_A$. Quando essa função g existe (única, pois a composição é associativa), é chamada *inversa* da função f, sendo representada por f^{-1}. Nesse caso, dizemos que f é *inversível*.

Por exemplo, se V é o conjunto das vogais, a função $f \in \mathfrak{I}(V)$, $f = \{(a, e), (e, i), (i, o), (o, u), (u, a)\}$ é inversível e $f^{-1} = \{(e, a), (i, e), (o, i), (u, o), (a, u)\}$. De fato,

$$(f \circ f^{-1})(a) = f(f^{-1}(a)) = f(u) = a,$$

$$(f \circ f^{-1})(e) = f(f^{-1}(e)) = f(a) = e,$$

$$(f \circ f^{-1})(i) = f(f^{-1}(i)) = f(e) = i,$$
$$(f \circ f^{-1})(o) = f(f^{-1}(o)) = f(i) = o,$$
$$(f \circ f^{-1})(u) = f(f^{-1}(u)) = f(o) = u,$$

o que mostra que $f \circ f^{-1} = I_V$. Como também (o que é muito fácil verificar) $f^{-1} \circ f = I_V$, temos que f é inversível.

Por seu turno, a função g de $\mathfrak{I}(V)$, $g = \{(a, u), (e, u), (i, u), (o, u), (u, u)\}$ não é inversível pois para que $(g^{-1} \circ g)(a) = a$ e $(g^{-1} \circ g)(e) = e$ dever-se-ia ter $g^{-1}(u) = a$ e $g^{-1}(u) = e$ e g^{-1} não seria uma função.

O conceito de *inversibilidade de função* pode ser facilmente generalizado para as funções do conjunto $\mathfrak{I}(A, B)$, dados dois conjuntos A e B. Dizemos que uma função $f \in \mathfrak{I}(A, B)$ é *inversível* se existe uma função $g \in \mathfrak{I}(B, A)$ tal que $f \circ g = I_B$ e $g \circ f = I_A$. Nesse caso, e como acima, diz-se que g é a *função inversa* de A e indica-se g por f^{-1}.

Por exemplo, se V é o conjunto das vogais e $C = \{b, c, d, f, g\}$, a função $f = \{(a, b), (e, c), (i, d), (o, f), (u, g)\}$, de V em C é claramente inversível e $f^{-1} = \{(b, a), (c, e), (d, i), (f, o), (g, u)\}$.

Observe que $f \in \mathfrak{I}(A, B)$ é inversível, então f^{-1} é única. De fato, se g_1 e g_2 são inversas de f temos

$$g_1 = I_A \circ g_1 = (g_2 \circ f) \circ g_1 = g_2 \circ (f \circ g_1) = g_2 \circ I_B = g_2,$$

onde utilizamos a observação do final da seção anterior e as igualdades $f \circ g_1 = I_B$ e $g_2 \circ f = I_A$ decorrentes da hipótese de que g_1 e g_2 eram inversas de f.

Além de f^{-1} ser única ela também é inversível pois, sendo $f \circ f^{-1} = I_B$ e $f^{-1} \circ f = I_A$, temos que $(f^{-1})^{-1} = f$.

Nos exemplos apresentados, concluímos a inversibilidade ou não de uma função procurando a sua função inversa. Vamos mostrar uma forma de analisar a inversibilidade de uma função sem nos preocuparmos com a inversa (na maioria das vezes, além de precisarmos apenas saber se a função é inversível, a determinação da inversa de uma função não é tarefa simples). Para isso, necessitamos de algumas definições.

Uma função $f \in \mathfrak{I}(A, B)$ é dita

i) *injetiva* (ou *injetora* ou uma *injeção*) se $x_1 \neq x_2$ implicar $f(x_1) \neq f(x_2)$.

Em outros termos, em uma função injetiva objetos diferentes têm sempre imagens diferentes. Ou ainda, em uma *função injetiva* de $\mathfrak{I}(A, B)$ não existe elemento de B que seja imagem de dois objetos distintos. Portanto, se f é injetiva e $f(x_1) = f(x_2)$, então $x_1 = x_2$, o que é uma outra forma de se caracterizar a injetividade.

Por exemplo, se V é o conjunto das vogais e $B = \{b, c, d, f, g\}$, a função $f = \{(a, b), (e, c), (i, d), (o, f), (u, g)\}$ é claramente injetiva,

enquanto que a função $g = \{(a, b), (e, b), (i, d), (o, d), (u, g)\}$ não o é, pois $g(a) = g(e)$. Obviamente, se g é uma *restrição* de $f \in \mathfrak{I}(A, B)$ a um subconjunto de A e f é injetora, então g também é injetora.

ii) *sobrejetiva* (ou *sobrejetora* ou *sobre* ou, ainda, uma *sobrejeção*) se $f(A) = B$.

Em outros termos, uma função é sobrejetiva se todo elemento do contradomínio é imagem de algum objeto. A função f do exemplo anterior é sobrejetiva enquanto a função g não o é, pois $c \notin g(A)$.

iii) *bijetiva* (ou *bijetora* ou uma *bijeção*) se ela é simultaneamente *injetora* e *sobrejetora*.

Uma propriedade das funções bijetivas que será útil posteriormente é a seguinte:

Sejam X e Y dois conjuntos, a um elemento de X e b um elemento de Y. Se existir uma função bijetiva f de X em Y, com $b \neq f(a)$, então existe uma função bijetiva g de X em Y tal que $g(a) = b$.

De fato, como f é sobrejetiva e b é um elemento de Y, existe $a' \in X$ tal que $b = f(a')$. Se definirmos g de X em Y por $g(a) = b$, $g(a') = b'$, com $b' = f(a)$, e $g(x) = f(x)$ se $x \neq a$ e $x \neq a'$, temos que g é bijetiva, pois a única diferença entre f e g está no fato de que $(a', b), (a, b') \in f$ enquanto $(a', b'), (a, b) \in g$.

A inversibilidade de uma função pode ser verificada sem que

se determine a sua inversa, como mostra a seguinte propriedade.

Uma função $f \in \mathcal{F}(A, B)$ é inversível se e somente se f é bijetiva.

Para provar, suponhamos inicialmente que f é bijetora e provemos que f é inversível. Seja g a função de B em A definida por $g(y) = x$, onde x é tal que $f(x) = y$. Como f é sobrejetora, para todo $y \in B$ existe $x \in A$ tal que $y = f(x)$. Além disso, este x é único pois f é injetiva. Assim g está bem definida (ou seja, é realmente uma função) e $(f \circ g)(y) = f(g(y)) = f(x) = y$, o que mostra que $f \circ g = I_B$. Do mesmo modo, $(g \circ f)(x) = g(f(x)) = g(y) = x$, o que mostra que $g \circ f = I_A$. Assim, f é inversível.

Reciprocamente, suponhamos que f é inversível e provemos que f é bijetiva. Para mostrar que f é injetiva, suponhamos $x_1, x_2 \in A$ com $f(x_1) = f(x_2)$. Temos $f^{-1}(f(x_1)) = f^{-1}(f(x_2))$ e, portanto, $x_1 = x_2$, provando o que queríamos. Para provar que f é sobrejetiva, seja $y \in B$ e provemos que existe $x \in A$ tal que $y = f(x)$. Como existe a função f^{-1}, temos que existe $x \in A$ tal que $x = f^{-1}(y)$ e então $f(x) = f(f^{-1}(y)) = I_B(y) = y$, concluindo o que queríamos provar.

Observe que uma função bijetiva de um conjunto A em um conjunto B e sua inversa (de B em A) estabelecem uma correspondência entre os elemento dos dois conjuntos: cada elemento

a de *A* é relacionado com um único elemento *b* de *B* (através da função *f*) que, por sua vez, é associado, de maneira única, ao elemento *a* de *A* (através da inversa de *f*). Dizemos então que uma função bijetiva de um conjunto em outro estabelece uma *correspondência biunívoca* ou uma *correspondência um a um* entre os dois conjuntos.

1.19 Exercícios

Para receber propostas de soluções, basta enviar e-mail para jaime@ic.ufal.br com as seguintes informações: nome completo, categoria (discente/docente), curso, instituição, estado/cidade.

1.1. Verifique se cada uma das relações abaixo definidas no conjunto de habitantes da terra (com os significados usuais da linguagem comum) é reflexiva, simétrica, transitiva ou total.

a) "*x* é primo de *y*".

b) "*x* é filho de *y*".

c) "*x* ama *y*".

1.2. Verifique se a relação "*x* é chefe de *y*" definida no conjunto dos funcionários da Universidade Federal de Alagoas (com o significado usual da língua portuguesa) é reflexiva, simétrica, transitiva ou total.

1.3. Dê um exemplo de uma relação binária definida no conjunto $A = \{a, b, c\}$ que não seja reflexiva, seja simétrica e transitiva e não seja total.

1.4. Apresente um contraexemplo que mostre que a afirmação "se R é uma relação simétrica e transitiva, então R é reflexiva" é falsa.

1.5. Mostre que se p, q e r são predicados em um conjunto A, então

a) $p \wedge (q \vee r) = (p \wedge q) \vee (p \wedge r)$ (isto é, a conjunção é distributiva em relação à disjunção).

b) $p \vee (q \wedge r) = (p \vee q) \wedge (p \vee r)$ (isto é, a disjunção é distributiva em relação à conjunção).

1.6. Mostre que se p é um predicado em um conjunto A, então

a) $p \wedge (\sim p) = \gamma$.

b) $p \vee (\sim p) = \tau$.

1.7. Prove as *leis de Morgan*: se p e q são predicados em um conjunto A então

a) $\sim(p \wedge q) = (\sim p) \vee (\sim q)$.

b) $\sim(p \vee q) = (\sim p) \wedge (\sim q)$.

1.8. Sejam p e q predicados em um conjunto A. Mostre que $(p \Rightarrow q) = (\sim p) \vee q$.

1.9. Sejam p e q predicados em um conjunto A e γ uma contradição. Mostre que $(p \Rightarrow q) = ((p \wedge (\sim q)) \Rightarrow \gamma)$.

1.10. Sejam um universo U e A, B, C subconjuntos de U. Mostre que

a) $(A \cup B) \cup C = A \cup (B \cup C)$ (a união é associativa).

b) $A \cap B \subset A$.

c) $(A \cap B) \cap C = A \cap (B \cap C)$ (a interseção é associativa).

d) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ (a interseção é distributiva em relação à união).

e) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ (a união é distributiva em relação à interseção).

1.11. Encontre contraexemplos que neguem as seguintes afirmações.

a) Se $A \cup B = A \cup C$ então $B = C$.

b) Se $A \cap B = A \cap C$ então $B = C$.

1.12. Mostre que se $A \cup B = A \cup C$ e $A \cap B = A \cap C$, então $B = C$.

1.13. Escreva "se $A \cup B = A \cup C$ e $A \cap B = A \cap C$, então $B = C$" na linguagem matemática.

1.14. Sejam A, B e C três conjuntos, f uma função de A em B

e g uma função de B em C. Mostre que

a) Se f e g são injetoras, então $g \circ f$ é injetora.

b) Se f e g são sobrejetoras, então $g \circ f$ é sobrejetora.

c) Se f e g são bijetoras, então $g \circ f$ é bijetora.

d) Se $g \circ f$ é injetora, então f é injetora.

e) Se $g \circ f$ é injetora e f é sobrejetora, então g é injetora.

f) Se $g \circ f$ é sobrejetora, então g é sobrejetora.

g) Se $g \circ f$ é sobrejetora e g é injetora então f é sobrejetora.

h) Se f é bijetora, então f^{-1} é bijetora.

1.15. Apresente um contraexemplo que mostre que $g \circ f$ ser bijetora não implica f e g serem bijetoras.

2. Os números naturais

2.1 Axiomas, teorias axiomáticas, objetos construídos axiomaticamente

Vimos na seção 1.1 que alguns objetos matemáticos são admitidos de forma primitiva, não sendo definidos. Um conjunto é um ente primitivo, enquanto uma função não o é.

Uma outra forma de se conceber um objeto matemático é se estabelecer propriedades as quais ele deve satisfazer, independentemente de qualquer conceituação anterior. Nesse caso, tais propriedades são chamadas *axiomas* ou *postulados* e dizemos que tal objeto foi *construído axiomaticamente*.

Axiomas também são utilizados para o estabelecimento de teorias matemáticas. Para tal, objetos são concebidos de forma primitiva e se estabelecem as propriedades (os axiomas) que esses objetos devem satisfazer. Uma teoria assim obtida é dita uma *teoria axiomática* e o exemplo mais conhecido é a *Geometria Euclidiana*, que foi construída a partir dos entes primitivos *ponto*, *reta* e *plano* e de axiomas (chamados *Postulados de* Euclides) como os seguintes:

- Dois pontos distintos determinam uma única reta.

- Uma reta sempre contém dois pontos distintos.
- Existem três pontos que não pertencem a uma mesma reta.
- Por um ponto não pertencente a uma reta passa uma única reta que é paralela à reta dada.

Estabelecidos os entes primitivos e os axiomas de uma teoria, sua ampliação decorre da construção de outros objetos (por definição ou construção axiomática) a serem manipulados na teoria e do estabelecimento de propriedades gozadas pelos entes primitivos e pelos novos objetos definidos. Essas propriedades são estabelecidas em *lemas*, *proposições*, *teoremas* e *corolários*. Um *lema* é uma propriedade que não tem muita importância por si mesma, mas é básica para a demonstração de outras propriedades; um *teorema* é uma propriedade que tem extrema importância na teoria que está sendo desenvolvida ou tem importância histórica no desenvolvimento da Matemática como um todo; um *corolário* é uma consequência imediata de uma *proposição* (propriedade de importância mediana) ou de um *teorema.*

Considerando que lemas, proposições, teoremas e corolários não são axiomas, suas veracidades devem ser devidamente demonstradas.

2.2 O conjunto dos números naturais

Desde os primeiros anos do ensino fundamental, estamos acostumados a trabalhar com *números naturais*, associando-os sempre à ideia de quantidade e os utilizando para realizar contagens. Aprendemos a *somar* e a *multiplicar* tais números, mas não estabelecemos exatamente o que eles são. É o que faremos agora.

Vamos estabelecer axiomaticamente que o *conjunto dos números naturais* é o conjunto, indicado por $\mathbb{N}$, que satisfaz os seguintes axiomas, chamados *postulados de Peano*:

1. Existe uma função injetiva s de $\mathbb{N}$ em $\mathbb{N}$ (a função s é chamada *sucessor* e, para cada $n \in \mathbb{N}$, a imagem $s(n)$ é dita *sucessor de* n).

2. Em $\mathbb{N}$ existe um elemento, chamado *um* e indicado por 1, tal que $s(\mathbb{N}) = \mathbb{N} - \{1\}$.

3. Se um predicado p definido em $\mathbb{N}$ é tal que

   i) $p(1) = \text{V}$ e

   ii) se $p(n) = \text{V}$, então $p(s(n)) = \text{V}$,

então p é uma tautologia em $\mathbb{N}$.

Observe que o segundo axioma implica que $\mathbb{N} \neq \varnothing$ e que $s(1) \neq 1$. Assim, $\mathbb{N}$ possui elementos diferentes de 1. Representando por 2

(chamado *dois*) o natural $s(1)$ e por 3 (chamado *três*) o natural $s(2)$, temos que $3 \neq 2$, pois se $s(2) = 2$, s não seria injetiva já que $s(1) = 2$. Na verdade, provaremos adiante que $s(n) \neq n$, qualquer que seja $n \in \mathbb{N}$.

Utilizando as representações estabelecidas acima, representaremos o conjunto dos números naturais por $\mathbb{N} = \{1, 2, 3,...\}$, onde as reticências "substituem" $s(3) = 4$ (*quatro*), $s(4) = 5$ (*cinco*), $s(5) = 6$ (*seis*), $s(6) = 7$ (*sete*), $s(7) = 8$ (*oito*), $s(8) = 9$ (*nove*), $s(9) = 10$ (*dez*), $s(10) = 11$ (*onze*), $s(11) = 12$ (*doze*) e, assim, sucessivamente. O fato de utilizarmos o símbolo 1 repetido para representar o natural *onze* será explicado no capítulo 5.

Observe ainda que esse axioma implica que todo elemento $n \in \mathbb{N}$, $n \neq 1$, é sucessor de um natural m. Esse natural m é chamado *antecessor* de n e é indicado por $n - 1$ (como veremos adiante, o *sucessor* de n é indicado $n + 1$). Observe também que $s(n - 1) = n$.

O terceiro axioma é chamado *Princípio da Indução Matemática* e pode ser utilizado para demonstrar afirmações sobre números naturais: para se demonstrar uma afirmação sobre os números naturais, basta se provar que a afirmação é verdadeira para 1 e que se for verdadeira para um natural k, sê-lo-á para o natural $s(k)$. A condição (i) é chamada *base da indução* e a assunção $p(n) = V$ é chamada *hipótese de indução*.

Como mostra a proposição a seguir, o Princípio da Indução Matemática pode ser enunciado de uma outra forma, como fazem outros autores.

Proposição 1.2

O Princípio da Indução Matemática é equivalente à seguinte propriedade:

Se A é um subconjunto de $\mathbb{N}$ tal que $1 \in A$ e $n \in A$ implica $s(n) \in A$, então $A = \mathbb{N}$.

Demonstração

Provemos inicialmente que o Princípio da Indução Matemática implica a propriedade acima. Para isso, seja A um subconjunto de $\mathbb{N}$ tal que $1 \in A$ e $n \in A$ implica $s(n) \in A$. Considere o predicado p em $\mathbb{N}$ definido por $p(\mathrm{x}) = \mathrm{V}$ se $\mathrm{x} \in A$. De $1 \in A$ temos que $p(1) = \mathrm{V}$ e de $n \in A$ implica $s(n) \in A$ temos que $p(n) = \mathrm{V}$ implica $p(\mathrm{s}(n)) = \mathrm{V}$. Assim, pelo princípio da indução, p é uma tautologia em $\mathbb{N}$ e, portanto, $n \in A$ para todo $n \in \mathbb{N}$. Logo $A = \mathbb{N}$.

Provemos agora que a propriedade acima implica o Princípio da Indução Matemática. Seja então um predicado p em $\mathbb{N}$ tal que $p(1) = \mathrm{V}$ e se $p(k) = \mathrm{V}$, então $p(\mathrm{s}(k)) = \mathrm{V}$. Considere o conjunto $A = \{\mathrm{x} \in \mathbb{N} | \, p\}$. De $p(1) = \mathrm{V}$ segue que $1 \in A$ e de $p(\mathrm{k}) = \mathrm{V}$ implica $p(s(\mathrm{k})) = \mathrm{V}$ segue que $n \in A$ implica $s(n) \in A$. Assim, pela

propriedade, $A = \mathbb{N}$ e p é uma tautologia em $\mathbb{N}$.

2.3 Operações no conjunto dos números naturais

Como dissemos no início da seção anterior, desde a nossa tenra idade aprendemos a *somar* e *multiplicar* números naturais. Vamos formalizar o que isso significa.

Em $\mathbb{N}$ definimos as seguintes operações, considerando n e m números naturais:

i) *Adição* (operador: +, denominação: **mais**)

a) $n + 1 = s(n)$;

b) $n + (m + 1) = s(n + m)$.

ii) *Multiplicação* (operador: . ou ×, denominação: **vez(es)**)

a) $n \,.\, 1 = n$;

b) $n \,.\, (m + 1) = n \,.\, m + n$.

Observe que de acordo com o item *a* da definição da adição os itens *b* podem ser escritos: $n + s(m) = s(n + m)$ e $n \,.\, s(m) = n \,.\, m + n$.

É necessário se provar que essas operações são, de fato, operações em $\mathbb{N}$. Isto é, é necessário provar que se $m, n \in \mathbb{N}$, então $n + m \in \mathbb{N}$ e $n \,.\, m \in \mathbb{N}$. Para demonstrar a primeira afirmação, seja

$n \in \mathbb{N}$ e consideremos o predicado em $\mathbb{N}$ definido por $p(m) = V$ se $n + m \in \mathbb{N}$. Temos que $p(1) = V$, pois $n + 1 = s(n)$ e s é uma função de $\mathbb{N}$ em $\mathbb{N}$. Além disso, se $p(m) = V$, temos $n + m \in \mathbb{N}$ e então, como $n + s(m) = n + (m + 1) = s(n + m)$, temos $p(s(m)) = V$, pois, novamente, s é uma função de $\mathbb{N}$ em $\mathbb{N}$. Deixamos para o leitor verificar que esse raciocínio se aplica à multiplicação.

Exemplos

a) $1 + 1 = s(1) = 2$.

b) $2 + 1 = s(2) = 3$.

c) $1 + 2 = 1 + (1 + 1) = s(1 + 1) = s(2) = 3$.

d) $2 + 2 = 2 + (1 + 1) = s(2 + 1) = s(3) = 4$.

e) $1 \times 2 = 1 \times (1 + 1) = 1 \times 1 + 1 = 1 + 1 = 2$.

f) $2 \times 2 = 2 \times (1 + 1) = 2 \times 1 + 2 = 2 + 2 = 4$.

Observe que, do mesmo modo que $2 = 1 + 1 = 2$ e $3 = 2 + 1$, temos $4 = 3 + 1$, $5 = 4 + 1$, $6 = 5 + 1$, …, $12 = 11 + 1$.

Observe ainda que $3 = 2 + 1 = 1 + 1 + 1$, $4 = 3 + 1 = = 1 + 1 + 1 + 1$ e, assim, para um natural n qualquer, $n = 1 + 1 + \ldots + 1$, com o segundo membro contendo n parcelas, ou seja "*n vezes 1*". Isto justifica a denominação *vezes* para o operador da multiplicação.

Vale observar também que essas são as *operações* com números naturais que aprendemos nos primeiros anos do ensino

fundamental.

A imagem $n + m$ é chamada *soma* de n e m. Nesse caso, n e m são chamados *parcelas.* A imagem $n \,.\, m$ é chamada *produto* de n por m. Nesse caso, n e m são chamados *fatores*. Um produto do tipo $n \,.\, n$ pode ser representada por n^2 (lido *n ao quadrado*) e um produto do tipo $n \,.\, m$ pode ser indicado por nm se m não é um número natural específico, n não é o natural 1 e quando não houver perigo de restrição à clareza (ou seja, o produto $n \,.\, m$ pode ser indicado por $n \times m$ ou por nm).

Observe que o conceito de *antecessor* introduzido na seção anterior e a definição de adição implicam que se $n \neq 1$, então $(n - 1) + 1 = n$.

Para analisar a comutatividade, a associatividade e a existência de elemento neutro da adição e da multiplicação, necessitamos do seguinte lema.

Lema 1.2

Para todo $n \in \mathbb{N}$, temos

i) $n + 1 = 1 + n$;

ii) $n \,.\, 1 = 1 \,.\, n$.

Demonstração

i) Consideremos o predicado em $\mathbb{N}$ $p(n) = V$ se $n + 1 = 1 + n$.

Temos que $p(1) = V$ pois, evidentemente, $1 + 1 = 1 + 1$. Suponhamos agora que $p(n) = V$ e provemos, a partir daí, que $p(s(n)) = V$. De $p(n) = V$, temos $n + 1 = 1 + n$ e então $1 + s(n) = s(1 + n) = s(n + 1) = (n + 1) + 1 = s(n) + 1$ e, portanto, $p(s(n)) = V$. Assim, pelo Princípio da Indução Matemática, $p(n) = V$ para todo $n \in \mathbb{N}$.

ii) Consideremos o predicado em $\mathbb{N}$ $p(n) = V$ se $n \cdot 1 = 1 \cdot n$.

Temos que $p(1) = V$ pois, evidentemente, $1 \cdot 1 = 1 \cdot 1$. Suponhamos agora que $p(n) = V$ e provemos, a partir daí, que $p(s(n)) = V$. De $p(n) = V$, temos $n \cdot 1 = 1 \cdot n$ e então $s(n) \cdot 1 = s(n) = n + 1 = n \cdot 1 + 1 = 1 \cdot n + 1 = 1 \cdot s(n)$, onde, na última igualdade, utilizamos o item (b) da definição da multiplicação. Logo $p(s(n)) = V$.

Uma implicação imediata da igualdade $n + 1 = 1 + n$ é a inexistência de elemento neutro da adição. De fato, se existisse um natural e tal que $n + e = e + n = n$, para todo natural n, teríamos $1 + e = e + 1 = 1$, contrariando o segundo postulado de Peano. Por seu turno, as igualdades $n = n \cdot 1 = 1 \cdot n$ implicam que o natural 1 é o elemento neutro da multiplicação. Sobre as demais propriedades das operações temos a seguinte proposição.

Proposição 2.2

As operações adição e multiplicação são associativas e

comutativas e a multiplicação é distributiva em relação à adição. Isto é, para todos $n, m, p \in \mathbb{N}$, temos

i) $n + (m + p) = (n + m) + p$ (associatividade da adição);

ii) $n(m + p) = nm + np$ (distributividade da multiplicação em relação à adição);

iii) $n(mp) = (nm)p$ (associatividade da multiplicação);

iv) $n + m = m + n$ (comutatividade da adição);

v) $nm = mn$ (comutatividade da multiplicação);

Demonstração.

i) Sejam $n, m \in \mathbb{N}$ e consideremos o predicado em $\mathbb{N}$ $p(k) = \text{V}$ se $(n + m) + k = n + (m + k)$.

Temos $p(1) = \text{V}$, pois $(n + m) + 1 = \text{s}(n + m) = n + (m + 1)$, onde na última igualdade foi utilizada o item *b* da definição da adição.

Suponhamos que $p(k) = \text{V}$, ou seja, suponhamos que $(n + m) + k = n + (m + k)$, e provemos que $p(\text{s}(k)) = \text{V}$.

Temos $(n + m) + \text{s}(k) = \text{s}((n + m) + k) = \text{s}(n + (m + k)) =$
$= n + \text{s}(m + k) = n + (m + \text{s}(k))$.

ii) Sejam $n, m \in \mathbb{N}$ e consideremos o predicado em $\mathbb{N}$ $p(k) = \text{V}$ se $n(m + k) = nm + nk$.

Temos $p(1) = \text{V}$, pois $n(m + 1) = nm + n = nm + n \cdot 1$.

Suponhamos que $p(k) = \text{V}$, ou seja, suponhamos que $n(m + k) = nm + nk$, e provemos que $p(\text{s}(k)) = \text{V}$.

Temos $n(m + s(k)) = n \cdot s(m + k) = n((m + k) + 1) =$ $= n(m + k) + n = (nm + nk) + n = nm + (nk + n) = nm + n \cdot s(k)$.

iii) Sejam n, $m \in \mathbb{N}$ e consideremos o predicado em $\mathbb{N}$ $p(k) = V$ se $(nm)k = n(mk)$.

Temos $p(1) = V$, pois $(nm) \cdot 1 = nm = n(m \cdot 1)$.

Suponhamos que $p(k) = V$, ou seja, suponhamos que $(nm)k = n(mk)$, e provemos que $p(s(k)) = V$. Temos

$(nm) \cdot s(k) = (nm)k + (nm)$ (definição da multiplicação)

$(nm) \cdot s(k) = n(mk) + nm$ (hipótese indutiva)

$(nm) \cdot s(k) = n(mk + m)$ (distributividade "ao contrário")

$(nm) \cdot s(k) = n(m \cdot s(k))$ (definição da multiplicação)

iv) Seja $n \in \mathbb{N}$ e consideremos o predicado em $\mathbb{N}$ $p(m) = V$ se $n + m = m + n$.

Pelo lema 1.2, temos $p(1) = V$. Suponhamos que $p(m) = V$, ou seja, suponhamos que $n + m = m + n$, e provemos que $p(s(m)) = V$. Temos

$n + s(m) = n + (m + 1)$

$n + s(m) = (n + m) + 1$

$n + s(m) = (m + n) + 1$

$$n + s(m) = m + (n + 1)$$
$$n + s(m) = m + (1 + n)$$
$$n + s(m) = (m + 1) + n$$
$$n + s(m) = s(m) + n$$

v) Seja $n \in \mathbb{N}$ e consideremos o predicado em $\mathbb{N}$ $p(m) = V$ se $nm = mn$.

Pelo lema 1.2, temos $p(1) = V$. Suponhamos que $p(m) = V$, ou seja, suponhamos que $nm = mn$, e provemos que $p(s(m)) = V$.

Inicialmente, provemos que $(n + m)p = np + mp$, quaisquer que sejam os naturais n, m e p. Para isso, consideremos o predicado em $\mathbb{N}$ $q(k) = V$ se $(n + m)k = nk + mk$.

Temos que $q(1) = V$, pois $(m + n) \cdot 1 = m + n = m \cdot 1 + n \cdot 1$. Suponhamos que $q(k) = V$ e provemos que $q(s(k)) = V$. Temos

$$(m + n)(k + 1) = (m + n)k + m + n$$
$$(m + n)(k + 1) = mk + nk + m + n$$
$$(m + n)(k + 1) = mk + m + nk + n$$
$$(m + n)(k + 1) = m(k + 1) + n(k + 1)$$

Agora, voltando ao predicado p, temos

$$n(m + 1) = nm + n$$
$$n(m + 1) = mn + n$$
$$n(m + 1) = mn + 1 \cdot n$$
$$n(m + 1) = (m + 1)n$$

As propriedades mostradas acima, entre outras finalidades, servem para facilitar a determinação de resultados de operações. Por exemplo,

$3 + 4 = 4 + 3 = 4 + (2 + 1) = 4 + (1 + 2) = (4 + 1) + 2 =$
$= 5 + 2 = 5 + (1 + 1) = 6 + 1 = 7$

$2\times4 = 2\times(2 + 2) = 2\times2 + 2\times2 = 4 + 4 = 4 + (3 + 1) =$
$= (4 + 3) + 1 = 7 + 1 = 8.$

A prática diuturna permite memorizar os resultados das operações envolvendo os naturais de 1 a 9: são as *tabuadas* da adição e da multiplicação.

Observe que a distributividade da multiplicação em relação à soma, dada por $n(m + p) = nm + np$, foi algumas vezes utilizada do segundo membro para o primeiro. Quando se utiliza esta propriedade nesse sentido, se diz que se está *fatorando n* ou que se está *colocando n em evidência*.

Observe também que, como $m = 1 + 1 + \ldots + 1$, m vezes, a distributividade implica $mn = (1 + 1 + \ldots + 1)n = n + n + \ldots + n$, m vezes. Ou seja, um produto pode ser visto como uma soma de parcelas iguais.

Corolário 1.2

Se $n, m \in \mathbb{N}$, então $s(n) + m = n + s(m)$.

Demonstração

Temos $s(n) + m = (n + 1) + m = n + (1 + m) = n + (m + 1) =$
$= n + s(m)$.

Pela injetividade da função *sucessor* estabelecida no primeiro axioma de Peano, temos que $n + 1 = m + 1$ implica $m = n$. Na verdade, essa conclusão pode ser generalizada, de acordo com a seguinte proposição, chamada *lei do corte* (ou do *cancelamento*) *da adição*.

Proposição 3.2

Sejam $n, m, k \in \mathbb{N}$. Se $n + k = m + k$, então $n = m$.

Demonstração

Consideremos o predicado em $\mathbb{N}$ definido por $p(k) = V$ se $n + k = m + k$ implicar $n = m$.

Pela observação acima, temos que $p(1) = V$. Suponhamos que $p(k) = V$ e provemos que $p(s(k)) = V$. Ora, se $n + (k + 1) = m + (k + 1)$, temos, por associatividade, $(n + k) + 1 = (m + k) + 1$ e então, pelo primeiro axioma de Peano, $n + k = m + k$. Daí, pela hipótese de indução, $n = m$, provando que $p(s(k)) = V$.

2.4 Equações no conjunto dos números naturais

Para analisarmos uma lei do corte para a multiplicação e definirmos uma relação de ordem no conjunto dos números naturais,

consideremos a seguinte definição. Se x é uma indeterminada em $\mathbb{N}$ e n e m são números naturais, uma igualdade do tipo $n + x = m$ é chamada de uma *equação* em $\mathbb{N}$. Um natural r tal que $n + r = m$ é chamado *solução* da equação e se uma equação admitir uma solução ela é dita *solúvel*. Por exemplo, a equação $1 + x = 3$ é solúvel, sendo 2 uma das suas soluções.

Claramente, a solução de uma equação em $\mathbb{N}$ solúvel é única. De fato, se r e r' são soluções da equação $n + x = m$, temos $n + r = m$ e $n + r' = m$ o que implica, pela transitividade da igualdade, $n + r = n + r'$, advindo daí, pela lei do corte para adição, $r = r'$. Assim, 2 é **a** solução da equação $1 + x = 3$.

Sobre equações em $\mathbb{N}$, temos a seguinte proposição.

Proposição 4.2

Sejam $n, m \in \mathbb{N}$,

i) A equação $n + x = n$ não é solúvel.

ii) Se a equação $n + x = m$ for solúvel, então a equação $m + x = n$ não é solúvel.

iii) Se a equação $n + x = m$ for solúvel, então $s(n) = m$ ou a equação $s(n) + x = m$ é solúvel.

iv) Se a equação $n + x = s(m)$ não é solúvel, então a equação $n + x = m$ também não é.

v) Se a equação $n + x = m$ não for solúvel, então $n = m$

ou a equação $m + x = n$ é solúvel.

Demonstração

i) Se existisse r tal que $n + r = n$, teríamos $n + (r + 1) = n + 1$ o que implicaria, pela lei do corte, $r + 1 = 1$, contrariando o segundo axioma de Peano.

ii) Se as equações $n + x = m$ e $m + x = n$ fossem solúveis, existiriam naturais r e p tais que $n + r = m$ e $m + p = n$. Daí, $n + (r + p) = n$ e a equação $n + x = n$ teria solução.

iii) Seja k a solução da equação $n + x = m$. Se $k = 1$, temos $n + 1 = m$ e, portanto, $m = s(n)$. Se $k \neq 1$, temos $k = s(k - 1)$ e então $n + s(k - 1) = m$ o que implica, pelo corolário 1.2, $s(n) + (k - 1) = m$. Essa igualdade mostra que a equação $s(n) + x = m$ é solúvel.

iv) Se a equação $n + x = m$ fosse solúvel, existiria um natural r tal que $n + r = m$, o que implicaria $n + (r + 1) = m + 1$ e a equação $n + x = s(m)$ seria solúvel.

v) Seja $n \in \mathbb{N}$ e consideremos o predicado em $\mathbb{N}$ $p(m) = V$ se a equação $n + x = m$ não for solúvel, então $n = m$ ou a equação $m + x = n$ é solúvel.

Temos que $p(1) = V$, pois se $n + x = 1$ não for solúvel e tivermos $n \neq 1$, temos $1 + (n - 1) = n$ o que implica que a equação $1 + x = n$ é solúvel.

Suponhamos que $p(m) = V$ e provemos que $p(s(m)) = V$. Para

isto, suponhamos que a equação $n + x = s(m)$ não seja solúvel. Daí, pelo item (iv), a equação $n + x = m$ não é solúvel o que implica, pela hipótese de indução, $n = m$ ou $m + x = n$ é solúvel. Porém, $n \neq m$, pois, do contrário, $n + 1 = s(m)$, o que contraria a hipótese levantada acima de que a equação $n + x = s(m)$ não é solúvel. Logo, $m + x = n$ é solúvel e então, pelo item (iii), $s(m) = n$ ou $s(m) + x = n$ é solúvel, mostrando que $p(s(m)) = V$.

Observe que o item (i) da proposição acima implica que dado um natural n não existe um natural k tal que $n + k = n$. Dessa observação segue que $s(n) \neq n$, para todo natural n.

Agora temos condições de provar a lei do corte para a multiplicação.

Proposição 5.2

Se $n, m, p \in \mathbb{N}$ e $np = mp$, então $n = m$.

Demonstração

Pela proposição anterior, se $n \neq m$, uma das equações $n + x = m$ ou $m + x = n$ seria solúvel. Se existisse um natural r tal $n + r = m$, teríamos $(n + r)p = mp$ o que implicaria $np + rp = mp$ e a equação $np + x = mp$ seria solúvel, contrariando o item (i) da proposição anterior, pois, por hipótese, $np = mp$. Como é evidente que esse raciocínio se aplica à possibilidade de que a equação $m + x = n$ seja solúvel, temos que $n = m$.

2.5 Uma relação de ordem no conjunto dos números naturais

No capítulo anterior, estudamos relações definidas em um conjunto e estabelecemos quando uma relação é dita reflexiva, simétrica, antissimétrica, transitiva e total. Ficou estabelecido também que uma relação em um conjunto que é reflexiva, antissimétrica, transitiva e total é chamada uma relação de ordem. Vamos definir uma relação de ordem no conjunto dos naturais, formalizando as ideias de maior e menor aprendidas desde criança.

No conjunto dos números naturais definimos uma relação, chamada *menor do que ou igual a* e indicada pelo símbolo $\leq$, por:

$n \leq m$ se $n = m$ ou a equação $n + x = m$ é solúvel.

Observe que, como a solubilidade da equação $n + x = m$ implica a existência de um natural r tal que $n + r = m$, a relação $\leq$ poderia ser definida da seguinte forma:

$n \leq m$ se $n = m$ ou existe um natural r tal que $n + r = m$.

Proposição 6.2

A relação $\leq$ é uma *relação de ordem*. Isto é, $\leq$ é reflexiva,

antissimétrica, transitiva e total.

Demonstração

Sejam a, b e c números naturais quaisquer. Pela própria definição da relação, se $a = b$, temos $a \leq b$. Assim, $a \leq a$ e a relação é *reflexiva*.

Suponhamos agora que $a \leq b$ e $b \leq a$. Se a e b fossem diferentes, as equações $a + x =$ b e $b + x = a$ seriam solúveis o que contrariaria a proposição 4.2. Assim, $a = b$ e a relação é antissimétrica.

Se $a \leq b$ e $b \leq c$, temos $a = b$ ou existe um natural p tal que $a + p = b$ e $b = c$ ou existe um natural r tal que $b + r = c$. Daí, $a = c$ ou $a + (r + p) = c$, o que mostra que $a \leq c$. Assim, $\leq$ é *transitiva*.

Finalmente, a proposição 4.2 garante que $a = b$ ou $a + x = b$ é solúvel ou $b + x = a$ é solúvel. Ou seja, $a \leq b$ ou $b \leq a$ e $\leq$ é total.

Além de ser uma relação de ordem, a relação $\leq$ satisfaz as seguintes propriedades.

Proposição 7.2

Sejam n, $m \in \mathbb{N}$ tais que $n \leq m$. Então, para todo natural p, $n + p \leq m + p$ e $np \leq mp$.

Demonstração

De $n \leq m$ segue que $n = m$ ou existe um natural r tal que $n + r = m$. De $n = m$ segue que $n + p = m + p$ e $np = mp$. De $n + r = m$

segue que $n + (r + p) = m + p$ e $np + rp = mp$, que implicam $(n + p) + r = m + p$ e $np + rp = mp$. Logo, $n + p \leq m + p$ e $np \leq mp$.

Quando dois naturais n e m são tais que $n \leq m$ e $n \neq m$ dizemos que n *é* menor do que m e indicamos por $n < m$. Observe que, como as condições "$n = m$" e "a equação $n + x = m$ é solúvel" são incompatíveis, dizer que $n < m$ implica que a equação $n + x = m$ é solúvel. Ou seja, $n < m$ se e somente se existe um natural r tal que $n + r = m$. Observe que se $n \neq 1$, como $1 + (n - 1) = n$, $1 < n$, Observe também que $<$ pode ser vista como uma relação binária em $\mathbb{N}$ que é transitiva (ver exercício 2.9).

Também usamos $m \geq n$ (lido *m maior do que ou igual a n*) para indicar que $n \leq m$ e $m > n$ (lido *m maior que n*) como sinônimo de $n < m$. Como as relações $\leq$ e $<$ são transitivas, quando tivermos $n \leq m$ e $m \leq p$, podemos escrever $n \leq m \leq p$ e quando tivermos $n < m$ e $m < p$, podemos escrever $n < m < p$, caso em que dizemos que *m está entre n* e p. Qualquer uma das relações $<$, $\leq$, $>$, $\geq$ e $\neq$ é chamada *desigualdade.*

É interessante observar, como mostra a proposição a seguir, que não existe número natural entre um natural e o seu sucessor.

Proposição 8.2

Sejam n e m números naturais. Se $m > n$, então $m \geq n + 1$.

Demonstração

Se existisse um natural m tal que $m > n$ e $m < n + 1$, existiriam naturais r e p tais que $n + \mathrm{r} = m$ e $m + p = n + 1$, de onde seguiria que $n + (\mathrm{r} + p) = n + 1$. Daí, pela lei do corte, teríamos $r + p = 1$. Porém, a existência de naturais r e p tais que $r + p = 1$ é uma contradição, pois, se $p = 1$, $r + 1 = 1$ e se $p \neq 1$, $(r + (p - 1)) + 1 = 1$, que contraria o segundo axioma de Peano.

O conjunto dos números naturais satisfaz uma outra propriedade que será importante no sentido de relacionar o conjunto dos números naturais com contagens. Para sua demonstração necessitamos da seguinte proposição.

Proposição 9.2

Sejam $n, m \in \mathbb{N}$. Então

i) $1 \leq n$;

ii) $n < \mathrm{s}(n)$;

iii) Se $n < \mathrm{s}(m)$, então $n \leq m$.

Demonstração

i) Se $n \neq 1$, como $1 + (n - 1) = n$, temos $1 < n$. Logo, $1 \leq n$.

ii) Decorre imediatamente da igualdade $n + 1 = \mathrm{s}(n)$.

iii) Por contradição, suponhamos que $m < n$. Daí a equação $m + \mathrm{x} = n$ é solúvel e então, pela proposição 4.2, $\mathrm{s}(m) = n$ ou a equação $\mathrm{s}(m) + \mathrm{x} = n$ é solúvel. Assim $\mathrm{s}(m) \leq n$, contrariando a hipótese de que

$n < s(m)$.

Observe que o item (ii) dessa proposição e a transitividade da relação < implicam que $1 < 2 < 3 < \ldots < 9 < \ldots$ Daí ser natural (no sentido usual do termo) a representação do conjunto dos números naturais por $\mathbb{N} = \{1, 2, 3, ...\}$.

Observe também que o mesmo item (ii) mostra que $n < n + 1$ e, dessa forma, o início da demonstração da proposição poderia ser escrito: "Se existisse um natural m tal que $n < m < n + 1$ existiram naturais..."

Proposição 10.2 (Princípio da Boa Ordenação (PBO))

Se M é um subconjunto dos números naturais não vazio, então existe $p \in M$ tal que $p \leq m$ qualquer que seja $m \in M$.

Demonstração

Consideremos o conjunto $L = \{x \in \mathbb{N} | \ m \in M \Rightarrow x \leq m\}$. Observe que o item (i) da proposição anterior implica que $1 \in L$. Além disso, como pelo item (ii) da mesma proposição $s(k) > k$, para todo natural k, temos que se $m \in L$, então $s(m) \notin L$. Isto mostra que $L \neq \mathbb{N}$ e, então, a proposição 1.2 garante que existe $p \in L$ tal que $s(p) \notin L$. Logo, existe $t \in M$ tal que $t < s(p)$. Como o último item da proposição anterior garante que $t \leq p$ e as pertinências $p \in L$ e $t \in M$ implicam $p \leq t$, temos $p = t$. Assim, $p \in M$ e $p \leq m$, qualquer

que seja $m \in M$, já que $p \in L$.

O elemento p da proposição anterior é chamado *menor elemento* ou *elemento mínimo* de M.

2.6 Conjuntos finitos

Como dissemos no início da seção 2.2, aprendemos a manipular números naturais associando-os a quantidades e realizando contagens. Nesta seção, vamos formalizar estas ideias.

Dado $n \in \mathbb{N}$, seja $I_n = \{x \in \mathbb{N} | x \leq n\}$. Dizemos que um conjunto A é *finito* se $A = \varnothing$ ou existem um natural n e uma bijeção de I_n em A (ou, por inversibilidade, uma bijeção de A em I_n). Por exemplo, o conjunto $A = \{a, b, c\}$ é um conjunto finito pois, trivialmente, existe uma função bijetiva do conjunto $I_3 = \{1, 2, 3\}$ em A: f = {(1, a), (2, b), (3, c)}. Evidentemente, para cada $n \in \mathbb{N}$, o conjunto I_n é finito, pois a identidade é uma bijeção de I_n em I_n. Se um conjunto A não é finito dizemos que ele é *infinito*.

Vamos mostrar que se A é finito, então o natural n é determinado pelo conjunto A e pela existência da bijeção de A em I_n. Esse fato decorre da seguinte propriedade dos conjuntos I_n.

Proposição 11.2

Seja $n \in \mathbb{N}$. Se A é um subconjunto próprio de I_n e f é uma função de A em I_n, então f não é bijetiva.

Demonstração

Seja $Y = \{x \in \mathbb{N} | \text{existem } A \subset I_x, A \neq I_x, \text{ e uma bijeção } f \text{ de } A \text{ em } I_x\}$. Devemos provar que $Y = \varnothing$. Por contradição, suponhamos que $Y \neq \varnothing$. Assim, pelo Princípio da Boa Ordenação, Y tem um menor elemento m e, portanto, há um subconjunto próprio A de I_m tal que existe uma bijeção f de A em I_m. Se $m \in A$, por uma propriedade apresentada na seção 1.16, existe uma função bijetiva g de A em I_m, com $g(m) = m$ e a restrição g ao conjunto $A - \{m\}$ é uma bijeção de $A - \{m\}$ em I_{m-1}, o que contraria o fato de que m é o elemento mínimo de Y. Se $m \notin A$, seja $a \in A$ tal que $m = f(a)$. Assim, a restrição de f ao conjunto $A - \{a\}$ é uma bijeção de $A - \{a\}$ em I_{m-1}, o que contraria também o fato de que m é o elemento mínimo de Y.

Corolário 3.2

Seja A um conjunto finito não vazio. Se existem naturais n e m e bijeções f de A em I_n e g de I_m em A, então $n = m$.

Demonstração

Como g de I_m em A e f de A em I_n são bijetivas, as funções $f \circ g$, de I_m em I_n, e $(f \circ g)^{-1}$, de I_n em I_m, são bijetivas. Se $m < n$, I_m é subconjunto próprio de I_n e a função $f \circ g$ contrariaria a proposição

anterior. Do mesmo modo a função $(f \circ g)^{-1}$ contrariaria a citada proposição se $n < m$. Logo $n = m$.

Se A é um conjunto finito não vazio, o único natural n definido pela existência do subconjunto I_n e da bijeção de I_n em A é chamado *cardinalidade* de A ou *número de elementos* de A, indicado por $|A|$ ou $n(A)$. Dizemos também que A tem *n elementos*, sendo a obtenção deste número uma *contagem* dos elementos de A. Na prática, a obtenção de n (ou seja, a contagem dos elementos de um conjunto finito) é feita associando-se o natural 1 a um dos elementos, 2 a outro elemento, 3 a um outro elemento e, assim, sucessivamente: 1, 2, 3, etc. De modo semelhante, um conjunto finito não específico de cardinalidade n pode ser representado por $A = \{a_1, a_2, a_3, \ldots, a_n\}$.

Claramente, se A e B são dois conjuntos finitos *disjuntos* (isto é, $A \cap B = \varnothing$), então $|A \cup B| = |A| + |B|$ (ver exercício 2.11). Esse fato é utilizado para o ensino inicial de somas de números naturais: para se explicar que 2 + 3 = 5, toma-se um conjunto com duas laranjas e um outro conjunto com três laranjas e mostra-se que a união dos dois conjuntos terá cinco laranjas.

O corolário a seguir é conhecido como *princípio da casa dos pombos* ou *princípio das gavetas* e formaliza matematicamente um fato bastante intuitivo: se em um pombal existem mais pombos que casas, pelo menos uma casa deverá abrigar mais de um pombo; se

existirem mais casas do que pombos, pelo menos uma das casas ficará desocupada.

Corolário 4.2

Sejam A e B dois conjuntos finitos e f uma função de A em B. Se $|A| \neq |B|$, então f não é bijetiva.

Demonstração

Sejam $n = |A|$ e $m = |B|$. Assim, existem funções bijetivas g de I_n em A e h de B em I_m. Se $n < m$ e a função f de A em B fosse bijetiva, a função $h \circ f \circ g$ seria uma função bijetiva de I_n em I_m, contrariando a proposição 10.2, já que se $n < m$, então I_n é subconjunto próprio de I_m. Com raciocínio semelhante chegaríamos a uma contradição se $m < n$.

Concluímos este capítulo discutindo a "finitude" do conjunto dos números naturais.

Corolário 5.2

O conjunto dos números naturais é infinito.

Demonstração

Se $\mathbb{N}$ fosse finito, haveria um número natural n e uma bijeção f de $\mathbb{N}$ em I_n e a restrição de f ao conjunto I_{n+1} seria uma bijeção de I_{n+1} em $f(\mathbb{N} - I_{n+1})$, o que contrariaria a proposição 4.2, considerando que $f(\mathbb{N} - I_{n+1}) \subset I_n \subset I_{n+1}$ e $I_n \neq I_{n+1}$.

2.7 Exercícios

Para receber propostas de soluções, basta enviar e-mail para jaime@ic.ufal.br com as seguintes informações: nome completo, categoria (discente/docente), curso, instituição, estado/cidade.

2.1. Dê exemplo de uma função sobrejetiva de $\mathbb{N}$ em $\mathbb{N}$ diferente da função identidade.

2.2. Considere o seguinte predicado definido em $\mathbb{N}$: $p(n) = \text{V}$ se n é número pequeno.

Temos que $p(1) = \text{V}$, pois 1 é um número pequeno. Além disso, se $p(n) = \text{V}$, é óbvio que $p(\text{s}(n)) = \text{V}$, pois se n é um número pequeno, então $n + 1$ é um número pequeno. Assim, pelo princípio da indução, *todo número natural é pequeno*. O que há de errado com essa "demonstração"?

2.3. Mostre que, quaisquer que sejam os naturais a e b,

a) $2a = a + a$.

b) $(a + b)^2 = a^2 + 2ab + b^2$.

2.4. Mostre que a relação definida em $\mathbb{N}\text{x}\mathbb{N}$ por $(m, n) \approx (p, q)$ *se e somente se* $m + q = n + p$ é uma relação de equivalência.

2.5. Mostre que, qualquer que seja o natural n,

a) $1 + 3 + ... + (2n - 1) = n^2$.

b) $2 + 4 + ... + 2n = n(n + 1)$.

2.6. Em $\mathbb{N}$ definamos a operação $n \otimes m = n + m + nm$. Mostre que $\otimes$ é comutativa, associativa e não possui elemento neutro.

2.7. Representemos por $n - m$ a solução da equação solúvel $m + x = n$ e consideremos um natural p ($n - m$ é chamada *subtração de n por m*). Mostre que

a) $n - m = (n + p) - (m + p)$.

b) Se $n - m = p$, então $n - p = m$.

c) $(n - m)p = np - mp$.

d) Se $n = m + p$, então $n - p = m$.

2.8. Sejam $a, b, c, d \in \mathbb{N}$. Mostre que

a) Se $a + c \leq b + c$, então $a \leq b$.

b) Se $a \leq b$ e $c \leq d$, então $a + c \leq b + d$.

2.9. Sejam $a, b, c \in \mathbb{N}$. Mostre que

a) Se $a < b$ e $b < c$, então $a < c$.

b) Se $a < b$ e $b \leq c$, então $a < c$.

c) Se $a < b$, então $a + c < b + c$.

d) Se $a < b$, então $ac < bc$.

e) Se $ac \leq bc$, então $a \leq b$

2.10. Mostre que se k e j são números naturais tais que

$kj = 1$, então $k = j = 1$.

2.11. No conjunto dos números naturais definimos a relação *b divide a* por "$b|a$ se e somente se existe um natural q tal que $a = bq$".

Mostre que essa relação é reflexiva, não é simétrica, é antissimétrica e é transitiva.

2.12. Sejam A e B são dois conjuntos finitos e não vazios. Mostre que

a) Se A e B são *disjuntos* (isto é, $A \cap B = \varnothing$), então $|A \cup B| = |A| + |B|$.

b) Se A e B não são *disjuntos*, então $|A \cup B| = |A| + |B| - |A \cap B|$.

2.13 Sejam A, B e C três conjuntos, com B e C disjuntos. Mostre que $A\text{x}(B \cup C) = (A\text{x}B) \cup (A\text{x}C)$.

2.14. Sejam A e B dois conjuntos finitos e não vazios. Mostre que $|A\text{x}B| = |A|.|B|$.

3. Os números inteiros

3.1 Introdução

No capítulo anterior, introduzimos a noção de equação no conjunto dos números naturais e vimos que uma equação $n + x = m$ tem solução se e somente se $n < m$ (na relação de ordem definida nos naturais). Há situações na prática em que necessitamos investigar uma equação do tipo $n + x = m$, com $n > m$. Um exemplo bem simples é o seguinte. Uma criança, cuja mesada é administrada pela mãe, tem um saldo de R$ 3,00. Se ela convence a mãe a comprar um sorvete que custa R$ 5,00, ela fica devendo (para ser descontado da mesada do próximo mês) R$ 2,00. A questão é: como expressar numericamente esse débito em relação ao saldo da sua mesada? Para que possamos fazer isto é necessário "ampliarmos" o conjunto dos números naturais, para chegarmos ao nosso velho conhecido conjunto dos números inteiros.

A partir dos números naturais, o conjunto dos inteiros pode ser construído através de definições. Vamos optar, por enquanto, em construir os inteiros também de forma axiomática, deixando o estabelecimento dos inteiros por definição para o capítulo 8. Essa

opção se deve ao fato de que as definições necessárias, embora fáceis, requerem uma maior maturidade matemática.

Uma outra razão para construirmos os inteiros axiomaticamente é que, nessa construção, o Princípio da Indução Matemática agora será um teorema enquanto o Princípio da Boa Ordenação será um axioma, ao contrário da construção axiomática dos números naturais. Essa mudança permitirá uma nova maneira de ver as coisas.

Além disso, a construção axiomática dos inteiros requer o estudo de algumas *estruturas algébricas*, que são também utilizadas em outros ramos da Matemática e na Ciência da Computação. Uma *estrutura algébrica* consiste em um conjunto munido de uma ou mais operações que satisfazem propriedades preestabelecidas. Estudaremos a estrutura chamada *anel* e algumas de suas "estruturas derivadas".

3.2 Anéis

Um *anel* é a estrutura algébrica que consiste em um conjunto A munido de duas operações, chamadas *adição* (operador: +, denominação: **mais**) e *multiplicação* (operador: **.** ou ×, denominação:

vez(es)), que satisfazem as seguintes propriedades.

(A_1) A adição é associativa: $a + (b + c) = (a + b) + c$, $\forall a, b, c \in A$.

(A_2) A adição é comutativa: $a + b = b + a$, $\forall a, b \in A$.

(A_3) A adição possui elemento neutro: $\exists e \in A$ tal que $a + e = a$, $\forall a \in A$.

(A_4) Todo elemento possui simétrico em relação à adição: $\forall a \in A$, $\exists a' \in A$ tal que $a + a' = e$.

(M_1) A multiplicação é associativa: $a \,.\, (b \,.\, c) = (a \,.\, b) \,.\, c$, $\forall a, b, c \in A$. (Quando não houver perigo de ambiguidades, omitiremos o operador da multiplicação, pondo os operandos justapostos: $a(bc) = (ab)c$, $\forall a, b, c \in A$; também poderemos omitir os espações entre os operandos e o operador: $a.(b.c) = (a.b).c$, $\forall a, b, c \in A$).

(M_2) A multiplicação é comutativa: $ab = ba$, $\forall a, b \in A$.

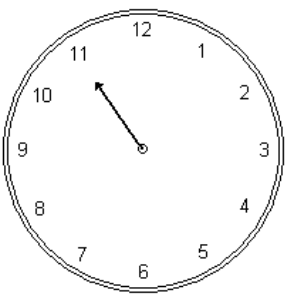
(M_3) A multiplicação possui elemento neutro: $\exists f \in A, f \neq e$, tal que $af = a$, $\forall a \in A$.

(AM) A multiplicação é distributiva em relação à adição: $a(b + c) = ab + ac$, $\forall a, b, c \in A$.

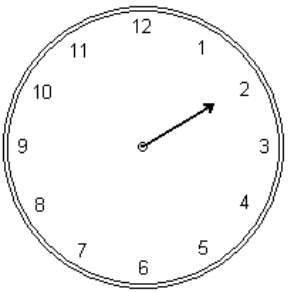
Normalmente, a referência a um anel genérico é feita apenas pela indicação do conjunto, ficando subentendidas as duas operações

adição e multiplicação. Quando necessário, indicaremos um anel por $(A, +, .)$, onde A é o conjunto, + e . são, respectivamente, as operações de adição e de multiplicação definidas no conjunto. Como nos naturais, uma imagem de uma adição $a + b$ é chamada *soma* e uma imagem de uma multiplicação $a \,.\, b$ é chamada *produto*. Na soma $a + b$, a e b são chamados *parcelas* e no produto $a \,.\, b$, a e b são chamados *fatores*. O produto $a \,.\, a$ pode ser indicado por a^2 (lido *a ao quadrado* ou *adois*).

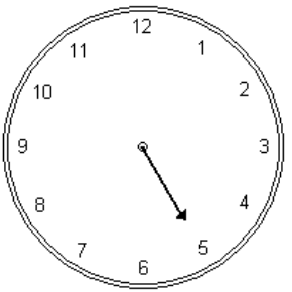
Para exemplificar, consideremos um mostrador de um relógio no instante em que o ponteiro das horas está sobre a marca das 11 horas.



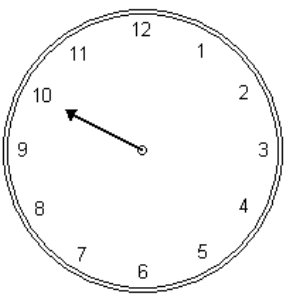
Três horas após este instante, o ponteiro estará sobre a marca das 2 horas:



Seis horas após aquele instante o ponteiro estará sobre 5 horas:



e 11 horas após, ele estará na marca das 10 horas.



De forma natural, podemos expressar esses fatos através de uma operação definida no conjunto $I_{12} = \{1, 2, 3, ..., 12\}$ pondo

$$11 + 3 = 2$$

$11 + 6 = 5$

$11 + 11 = 10$

Imagine agora que o ponteiro das horas esteja sobre a marcação das doze horas. Decorrido três vezes o intervalo de tempo de sete horas, o ponteiro ocupará a marca das nove horas o que justifica a igualdade $3 \cdot 7 = 9$.

Isso mostra (de forma natural, repetimos) que se pode definir uma adição e uma multiplicação em I_{12} de acordo com as seguintes tabelas, onde o elemento da linha i e da coluna j, representa $i + j$ na primeira e $i \cdot j$ na segunda.

Adição em I_{12}

+	1	2	3	4	5	6	7	8	9	10	11	12
1	2	3	4	5	6	7	8	9	10	11	12	1
2	3	4	5	6	7	8	9	10	11	12	1	2
3	4	5	6	7	8	9	10	11	12	1	2	3
4	5	6	7	8	9	10	11	12	1	2	3	4
5	6	7	8	9	10	11	12	1	2	3	4	5
6	7	8	9	10	11	12	1	2	3	4	5	6
7	8	9	10	11	12	1	2	3	4	5	6	7
8	9	10	11	12	1	2	3	4	5	6	7	8
9	10	11	12	1	2	3	4	5	6	7	8	9
10	11	12	1	2	3	4	5	6	7	8	9	10
11	12	1	2	3	4	5	6	7	8	9	10	11
12	1	2	3	4	5	6	7	8	9	10	11	12

Multiplicação em I_{12}

·	1	2	3	4	5	6	7	8	9	10	11	12
1	1	2	3	4	5	6	7	8	9	10	11	12
2	2	4	6	8	10	12	2	4	6	8	10	12
3	3	6	9	12	3	6	9	12	3	6	9	12
4	4	8	12	4	8	12	4	8	12	4	8	12
5	5	10	3	8	1	6	11	4	9	2	7	12
6	6	12	6	12	6	12	6	12	6	12	6	12
7	7	2	9	4	11	6	1	8	3	10	5	12
8	8	4	12	8	4	12	8	4	12	8	4	12
9	9	6	3	12	9	6	3	12	9	6	3	12
10	10	8	6	4	2	12	10	8	6	4	2	12
11	11	10	9	8	7	6	5	4	3	2	1	12
12	12	12	12	12	12	12	12	12	12	12	12	12

Talvez o leitor esteja pensando que é muito complicado executar essas operações. No capítulo 7, apresentaremos uma forma simples de realizá-las. Por enquanto, o ledor precisa observar apenas que $a + 12 = a$, para todo $a \in I_{12}$, o que mostra que 12 é elemento neutro da adição e que também a . $1 = a$, qualquer que seja $a \in I_{12}$, o que mostra que 1 é elemento neutro da multiplicação. Além disso, deve ser observado que as duas operações são claramente comutativas.

As demonstrações de que essas operações são associativas e que a multiplicação é distributiva em relação à adição requereriam que todos os casos possíveis fossem verificados, o que evidentemente seria extremamente desgastante. Na verdade, essas demonstrações são simples e serão feitas, em um caso geral, no capítulo 7. Por ora,

observe (lembrando que não são demonstrações, são apenas exemplos constatativos!) que:

$$(5 + 9) + 8 = 2 + 8 = 10,$$

$$5 + (9 + 8) = 5 + 5 = 10,$$

que

$$(5 \,.\, 8) \,.\, 9 = 4 \,.\, 9 = 12,$$

$$5 \,.\, (8 \,.\, 9) = 5 \,.\, 12 = 12$$

e que

$$5(7 + 3) = 510 = 2,$$

$$5 \,.\, 7 + 5 \,.\, 3 = 11 + 3 = 2.$$

É fácil ver também que todo elemento tem simétrico: o simétrico de 1 é 11, o simétrico de 2 é 10, o simétrico de 3 é 9 e assim por diante. Temos então que I_{12} munido dessas operações é um *anel*.

Para um outro exemplo, considere o conjunto dos dias da semana S = {Dom. Seg, Ter, Qua, Qui, Sex, Sab}, a operação definida no capítulo 1 (que agora vamos chamar de adição)

+	Dom	Seg	Ter	Qua	Qui	Sex	Sab
Dom	Seg	Ter	Qua	Qui	Sex	Sab	Dom
Seg	Ter	Qua	Qui	Sex	Sab	Dom	Seg
Ter	Qua	Qui	Sex	Sab	Dom	Seg	Ter
Qua	Qui	Sex	Sab	Dom	Seg	Ter	Qua
Qui	Sex	Sab	Dom	Seg	Ter	Qua	Qui
Sex	Sab	Dom	Seg	Ter	Qua	Qui	Sex
Sab	Dom	Seg	Ter	Qua	Qui	Sex	Sab

e a operação multiplicação dada na tabela

·	Dom	Seg	Ter	Qua	Qui	Sex	Sab
Dom	Dom	Seg	Ter	Qua	Qui	Sex	Sab
Seg	Seg	Qua	Sex	Dom	Ter	Qui	Sab
Ter	Ter	Sex	Seg	Qui	Dom	Qua	Sab
Qua	Qua	Dom	Qui	Seg	Sex	Ter	Sab
Qui	Qui	Ter	Dom	Sex	Qua	Seg	Sab
Sex	Sex	Qui	Qua	Ter	Seg	Dom	Sab
Sab	Sab	Sab	Sab	Sab	Sab	Sab	Sab

É exaustivo, mas é fácil (?!) ver que o conjunto dos dias da semana munido dessas operações é um anel. Por hora, observemos apenas que os elementos neutros da adição e da multiplicação são Sab e Dom, respectivamente e que o simétrico de Dom é Sex, o de Seg é Qui, e sucessivamente. (Como dissemos no capítulo 1, ainda neste capítulo mostraremos a lógica (no sentido usual do termo) que está por trás dessas operações).

(Pergunta para o leitor: o conjunto dos naturais construído no capítulo anterior munido das operações adição e multiplicação ali definidas é um anel?).

Em um anel qualquer, o elemento neutro (único, como mostrado na seção 1.13) da adição é chamado *zero* ou *elemento nulo* e é representado pelo símbolo 0. Observe que no anel I_{12} o elemento neutro da adição é 12 e, portanto, neste anel 0 = 12; no anel dos dias da semana 0 = Sab. Um elemento de um anel diferente do elemento neutro da adição é dito *não nulo*. Por sua vez, o elemento neutro

(único) da multiplicação é chamado *unidade* ou, simplesmente, *um* e é indicado por 1 (no anel dos dias da semana 1 = Dom). A soma 1 + 1 pode ser indicada por 2 (lido *dois*) e se a é um elemento do anel, o elemento $a + 1$ é chamado *consecutivo* ou *sucessor* de a (no anel dos dias da semana, o consecutivo de Seg é Ter (lógico, não?). Quando estivermos lidando com mais de um anel, poderemos adicionar índices aos símbolos 0 e 1 para indicar o anel respectivo.

Como a adição em um anel é associativa, o elemento simétrico de um elemento x do anel é único (conforme seção 1.12) e é representado por $-x$, chamado *menos x* (no anel I_{12}, por exemplo, -7 = 5; nos dias da semana, -Ter = Qua). Naturalmente, $x + (-x) = 0$. Uma adição do tipo $a + (-b)$ é indicada por $a - b$ e é chamada *subtração de a por b* ou *diferença entre a* e *b*.

Note que, como $a + (-a) = 0$, o elemento simétrico de - a é a. Ou seja, $-(-a) = a$. Observe também que o fato de $a = b$ implicar $a + c = b + c$, qualquer que seja o elemento c do anel, acarreta, se $a = b$, a seguinte sequência de igualdades:

$$a + (-b) = b + (-b),$$
$$a + (-b) = 0,$$
$$a - b = 0,$$

o que mostra que em todo anel vale a regra "muda de membro, muda de sinal". Observe que dessa propriedade decorre que se k é um

elemento de um anel tal que $k + k = k$, então $k = 0$.

A simples conceituação de anéis já gera propriedades interessantes, como mostram as proposições seguintes. A primeira delas é clássica: se um dos fatores de uma multiplicação é zero, o produto é igual a zero!

Proposição 1.3

Seja A um anel. Para todo $a \in A$, se tem $a \,.\, 0 = 0$.

Demonstração:

Temos

$a \,.\, 0 = a \,.\, (0 + 0)$ ($0 = 0 + 0$)

$a \,.\, 0 = a \,.\, 0 + a \,.\, 0$ (distributividade da multiplicação)

$a \,.\, 0 = 0$ (observação anterior: se $k + k = k$, então $k = 0$)

A próxima proposição estabelece o que, no futuro, poderá ser visto como "regras de sinais".

Proposição 2.3

Seja A um anel. Para todos $a, b \in A$,

a) $(-1) \,.\, a = -a$.

b) $(-a) \,.\, b = a \,.\, (-b) = -(ab)$.

c) $(-a) \,.\, (-b) = ab$.

Demonstração:

a) Pelo conceito de elemento simétrico, basta provar que $(-1) \cdot a + a = 0$. Temos

$(-1) \cdot a + a = (-1) \cdot a + 1 \cdot a$ $\quad (a = 1 \cdot a)$

$(-1) \cdot a + a = ((-1) + 1) \cdot a$ (colocando a em evidência)

$(-1) \cdot a + a = 0 \cdot a$ $\quad ((-1) + 1 = 0)$

$(-1) \cdot a + a = 0,$ (proposição anterior)

b) Temos $(-a) \cdot b = ((-1) \cdot a) \cdot b = (-1) \cdot (a \cdot b) = -(a \cdot b)$ e, para a outra igualdade, $a \cdot (-b) = (-b) \cdot a$ e, então, $a \cdot (-b) = -(ba) = -(ab)$.

c) A igualdade segue das seguintes aplicações do item (b) e do fato de que $-(-a) = a$: $(-a) \cdot (-b) = -(a \cdot (-b)) = -(-(ab)) = ab$.

3.3 Elementos inversíveis

Seja A um anel. Vamos discutir agora a existência de elemento simétrico em relação à multiplicação. Ou seja, vamos discutir o caso em que dado um elemento $a \in A$, existe $b \in A$ tal que $ab = 1$. Nesse caso, dizemos que a é *inversível* e b é chamado *inverso* de a. Como mostrado no capítulo1, o inverso de um elemento inversível a é único e é representado por a^{-1}.

No anel I_{12} do exemplo acima temos que 1, 5, 7 e 11 são

inversíveis ($1^{-1} = 1$, $5^{-1} = 5$, $7^{-1} = 7$ e $11^{-1} = 11$) e 0, 2, 3, 4, 6, 8, 9, 10 não são inversíveis. No anel dos dias da semana, todos os elementos não nulos são inversíveis. Por exemplo, $Seg^{-1} = Qua$ e $Ter^{-1} = Qui$.

Devido ao fato de que $a \,.\, 0 = 0$, para todo $a \in A$, conforme visto na proposição 1.3, o elemento neutro da adição de um anel nunca é inversível. Por sua vez, como $1 \,.\, 1 = 1$, o elemento neutro da multiplicação é sempre inversível e $1^{-1} = 1$. Como o item (c) da proposição 2.3 mostra que $(-1) \,.\, (-1) = 1 \,.\, 1 = 1$, temos que -1 é inversível e $(-1)^{-1} = -1$. Claramente, se a é inversível, a^{-1} também o é e $(a^{-1})^{-1} = a$.

3.4 Igualdade de anéis: anéis isomorfos

Como já foi dito e redito, ao se definir um novo ente matemático é necessário que se estabeleça quando dois representantes desse ente são considerados iguais. É o que faremos agora em relação a anéis.

Embora a igualdade de dois representantes de um ente matemático seja estabelecida por uma definição, é natural que essa definição vá ao encontro da lógica do senso comum. Nesse sentido, não havia sentido uma definição de igualdade de anéis que tornasse iguais os anéis I_{12} e o anel dos dias da semana. É razoável aceitar que

a igualdade de anéis deva passar pela "mesma cardinalidade" dos conjuntos envolvidos (o que pode ser exigido pela existência de uma função bijetiva) e da preservação das operações respectivas em relação aos objetos e suas imagens e vice-versa. Para atingir esse objetivo, consideremos a seguinte definição. Se $(A, +, .)$ e $(B, \#, *)$ são dois anéis, uma função bijetiva f de A em B é um *isomorfismo* (*de anéis*) se $f(a + b) = f(a) \# f(b)$, $f(a . b) = f(a) * f(b)$ e $f(1_A) = 1_B$.

Observe que um isomorfismo preserva as operações de adição e de multiplicação, no sentido de que o que acontece nos objetos, acontece nas imagens, atendendo parte da lógica explicitada acima. A proposição a seguir mostra que os outros parâmetros de um anel também são preservados por um isomorfismo.

Proposição 3.3.

Sejam $(A, +, .)$ e $(B, \#, *)$ dois anéis (com subtrações indicadas por – e ~, respectivamente) e f um isomorfismo de A em B . Então

a) $f(0_A) = 0_B$.

b) $f(-a) = \sim f(a)$, qualquer que seja $a \in A$.

c) $f(a - b) = f(a) \sim f(b)$, quaisquer que sejam $a, b \in A$.

Demonstração

a) Temos que $f(0_A) = f(0_A + 0_A) = f(0_A) \# f(0_A)$ e então, pela observação anterior à proposição 1.3, $f(0_A) = 0_B$.

b) Temos que $0_B = f(0_A) = f(a + (-a)) = f(a)\ \#\ f(-a)$ e então $f(-a) = \sim f(a)$.

c) Utilizando o item b, temos

$$f(a - b) = f(a + (-b)) = f(a)\ \#\ f(-b) = f(a) \sim f(b).$$

Falta apenas analisarmos a preservação das operações no sentido imagem/objeto: como mostra a seguinte proposição, um isomorfismo implica essa preservação através da sua função inversa,

Proposição 4.3

A função inversa de um isomorfismo de um anel A em um anel B é um isomorfismo de B em A.

Demonstração

Como f é um isomorfismo de A em B, f é bijetiva e, portanto, tem uma inversa f^{-1}. Sejam c e d dois elementos do anel B. Como f é bijetora existem únicos a e b em A tais que $f(a) = c$ e $f(b) = d$. Temos então $f^{-1}(c\ \#\ d) = f^{-1}(f(a)\ \#\ f(b)) = f^{-1}(f(a + b)) = a + b$ e, portanto, $f^{-1}(c\ \#\ d) = f^{-1}(c) + f^{-1}(d)$. Com demonstração idêntica se prova que $f^{-1}(c * d) = f^{-1}(c)\ .\ f^{-1}(d)$. Finalmente, a igualdade $f(1_A) = 1_B$ implica $f^{-1}(f(1_A)) = f^{-1}(1_B)$ e então $1_A = f^{-1}(1_B)$.

Dessa forma, a existência de um isomorfismo entre dois anéis implica que eles, mesmo que tenham elementos distintos e que as operações neles definidas sejam diferentes, algebricamente eles têm a mesma estrutura. Por essa razão, a existência de um isomorfismo

entre dois anéis é utilizada para definir igualdade de dois anéis: *dois anéis são iguais quando eles são isomorfos*.

Para um exemplo, consideremos o anel dos dias da semana S = {Dom. Seg, Ter, Qua, Qui, Sex, Sab}, com as operações

+	Dom	Seg	Ter	Qua	Qui	Sex	Sab
Dom	Seg	Ter	Qua	Qui	Sex	Sab	Dom
Seg	Ter	Qua	Qui	Sex	Sab	Dom	Seg
Ter	Qua	Qui	Sex	Sab	Dom	Seg	Ter
Qua	Qui	Sex	Sab	Dom	Seg	Ter	Qua
Qui	Sex	Sab	Dom	Seg	Ter	Qua	Qui
Sex	Sab	Dom	Seg	Ter	Qua	Qui	Sex
Sab	Dom	Seg	Ter	Qua	Qui	Sex	Sab

e

·	Dom	Seg	Ter	Qua	Qui	Sex	Sab
Dom	Dom	Seg	Ter	Qua	Qui	Sex	Sab
Seg	Seg	Qua	Sex	Dom	Ter	Qui	Sab
Ter	Ter	Sex	Seg	Qui	Dom	Qua	Sab
Qua	Qua	Dom	Qui	Seg	Sex	Ter	Sab
Qui	Qui	Ter	Dom	Sex	Qua	Seg	Sab
Sex	Sex	Qui	Qua	Ter	Seg	Dom	Sab
Sab	Sab	Sab	Sab	Sab	Sab	Sab	Sab

e o anel I_7 = {1, 2, 3, 4, 5, 7}, com as operações

+	1	2	3	4	5	6	7
1	2	3	4	5	6	7	1
2	3	4	5	6	7	1	2
3	4	5	6	7	1	2	3
4	5	6	7	1	2	3	4
5	6	7	1	2	3	4	5
6	7	1	2	3	4	5	6
7	1	2	3	4	5	6	7

e

·	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	4	6	1	3	5	7
3	3	6	2	5	1	4	7
4	4	1	5	2	6	3	7
5	5	3	1	6	4	2	7
6	6	5	4	3	2	1	7
7	7	7	7	7	7	7	7

e a função f de I_7 em S, $f(1)$ = Dom, $f(2)$ = Seg, $f(3)$ = Ter, $f(4)$ = Qua, $f(5)$ = Qui, $f(6)$ = Sex e $f(7)$ = Sab. Considerando que $1_{I_7} = 1$ e 1_S = Dom, já temos que $f(1_{I_7}) = 1_S$. Temos também (utilizando os mesmos operadores para representar as operações nos dois anéis):

$f(1 + 1) = f(2)$ = Seg e $f(1) + f(1)$ = Dom + Dom = Seg, ou seja, $f(1 + 1) = f(1) + f(1)$;

$f(1 + 2) = f(3)$ = Ter e $f(1) + f(2)$ = Dom + Seg = Ter, ou seja, $f(1 + 2) = f(1) + f(2)$;

...

$f(3 + 4) = f(7)$ = Sab e $f(3) + f(4)$ = Ter + Qua = Sab, ou seja,

$f(3 + 4) = f(3) + f(4)$;

...

$f(6 + 7) = f(6) =$ Sex e $f(6) + f(7) =$ Sex + Sab = Sex, ou seja, $f(6 + 7) = f(6) + f(7)$;

$f(7 + 7) = f(7) =$ Sab e $f(7) + f(7) =$ Sab + Sab = Sab, ou seja, $f(7 + 7) = f(7) + f(7)$;

e

$f(1 . 1) = f(1) =$ Dom e $f(1) . f(1) =$ Dom , Dom = Dom, ou seja, $f(1 . 1) = f(1) . f(1)$

...

$f(2 . 5) = f(3) =$ Ter e $f(2) . f(5) =$ Seg . Qui = Ter, ou seja, $f(2 . 5) = f(2) . f(3)$

...

Dessa forma, $f(x + y) = f(x) + f(y)$ e $f(x . y) = f(x) . f(y)$. Como já tínhamos observado que $f(1_{I_7}) = 1_S$, temos que f é um isomorfismo de I_7 em S e, portanto, esses anéis são iguais.

É dessa igualdade que segue a lógica das operações com os dias da semana, como prometemos na seção 3.2. Por exemplo, por que Ter + Qui = Dom? Se estivermos na terça-feira (3, em I_7), 5 (Qui em S) dias após iremos para o domingo (1, em I_7). E qual seria a lógica por trás da multiplicação do anel dias da semana? Resposta com o

leitor.

3.5 Domínios de integridade

Se o leitor observar a tabela de multiplicação do anel I_{12} e se lembrar que nesse anel 0 = 12, verificará, ao contrário do que estamos habituados, que 3 . 8 = 12. Ou seja, o produto de dois elementos não nulos é igual a zero! Observe que tal fato não ocorre no anel dos dias da semana (0 = Sab): $x \,.\, y = \text{Sab} \Leftrightarrow x = \text{Sab} \vee y = \text{Sab}$.

Definição: Um anel A é um *domínio de integridade* se a multiplicação do anel satisfizer a seguinte propriedade:

(M_4) Quaisquer que sejam $a, b \in A$, se $ab = 0$, então $a = 0$ ou $b = 0$.

Assim o anel I_{12} não é um domínio de integridade, pois, como já vimos, 3 . 8 = 0 e $3 \neq 0$ e $8 \neq 0$. Já o anel dos dias da semana é um domínio de integridade.

Vale observar (porque vamos eventualmente utilizar esta nova forma) que a propriedade (M_4) é claramente equivalente à seguinte propriedade.

(M_4') Quaisquer que sejam $a, b \in A$, se $a \neq 0$ e $b \neq 0$, então $ab \neq 0$.

Um domínio de integridade satisfaz a uma propriedade adicional, conhecida como *lei do cancelamento* ou *lei do corte*.

Proposição 5.3

Seja D um domínio de integridade. Quaisquer que sejam $a, b, c \in D$, se $a \neq 0$ e $ab = ac$, então $b = c$.

Demonstração

De $ab = ac$ segue que $ab + (-ac) = 0$ o que implica $ab + (a(-c)) = 0$. Daí, $a(b + (-c)) = 0$ e, então, como D é um domínio de integridade e $a \neq 0$, $b + (-c) = 0$ o que implica $b = c$.

Ao aplicarmos a lei do cancelamento em $ab = ac$ (se $a \neq 0$) obtendo $b = c$, dizemos que *dividimos* a igualdade $ab = ac$ por a ou que a igualdade $ab = ac$ foi *simplificada* por a.

3.6 Anéis ordenados

Vamos acrescentar a um anel uma relação binária (relação de ordem, como estudada no capítulo 1) que permitirá se fazer comparações (no sentido usual do termo) entre os elementos de um anel, dando-lhes uma ordenação (também no sentido usual do termo).

Definição: um anel A é dito *anel ordenado* se nele for definida uma relação de ordem (ou seja, uma relação binária reflexiva,

antissimétrica, transitiva e total), simbolizada por $\leq$, que satisfaz as seguintes propriedades.

a) *Compatibilidade com a adição*

Quaisquer que sejam $a, b, c \in A$, se $a \leq b$, então $a + c \leq b + c$.

b) *Compatibilidade com a multiplicação*

Quaisquer que sejam $a, b, c \in A$, se $a \leq b$ e $0 \leq c$, então $ac \leq bc$.

A expressão $x \leq y$ é lida *x é menor do que ou igual a y* e é equivalente à notação $y \geq x$, que é lida *y maior do que ou igual a x*.

Usamos a notação $x < y$ (que é lida *x menor do que y*) para indicar que $x \leq y$ e $x \neq y$. Da mesma forma, utilizamos $x > y$ (*x maior do que y*) significando que $x \geq y$ e $x \neq y$. Como $\leq$ é transitiva, podemos usar $x \leq y \leq z$ para indicar que $x \leq y$ e que $y \leq z$. Um exercício proposto (de fácil solução) mostrará que $x < y$ é também transitiva. Assim podemos usar $x < y < z$ para indicar que $x < y$ e $y < z$. Nesse caso, dizemos que *y está entre x e z*. Além da expressão $x \neq y$, qualquer das expressões $x \geq y$, $x \leq y$, $x > y$ e $x < y$ é chamada *desigualdade*.

Se $x > 0$, diz-se que x é *positivo* e se $x < 0$, diz-se que x é *negativo*. A positividade ou negatividade de um elemento de um anel ordenado também é citada como o *sinal* do elemento.

A multiplicação num anel ordenado satisfaz as propriedades

abaixo, que, combinadas com as propriedades estabelecidas na proposição 2.3, são conhecidas como *regras de sinais da multiplicação*.

Proposição 6.3

Sejam A um anel ordenado e a e b dois elementos de A.

a) Se $a \geq 0$, então $-a \leq 0$.

b) Se $a \leq 0$, então $-a \geq 0$.

c) Se $a \geq 0$ e $b \geq 0$, então $ab \geq 0$.

d) Se $a \geq 0$ e $b \leq 0$, então $ab \leq 0$.

e) Se $a \leq 0$ e $b \leq 0$, então $ab \geq 0$.

Demonstração:

a) Como $a \geq 0$, pela compatibilidade da relação de ordem com a adição, $a + (-a) \geq 0 + (-a)$ e então $0 \geq -a$.

b) Como $a \leq 0$, novamente pela compatibilidade da relação de ordem com a adição, $a + (-a) \leq 0 + (-a)$ e então $0 \leq -a$.

c) Decorre imediatamente da compatibilidade da relação de ordem com a multiplicação: $a \geq 0$ e $b \geq 0$ implica $ab \geq 0 \,.\, b$ e $0 \,.\, b = 0$.

d) Decorre também imediatamente da compatibilidade da relação de ordem com a multiplicação: $b \leq 0$ e $a \geq 0$ implica $ba \leq 0 \,.\, a$.

e) Como $a \leq 0$, pelo item (a), $-a \geq 0$. Aplicando a compatibilidade com a multiplicação a $b \leq 0$ e $-a \geq 0$ temos $b(-a) \leq 0 \ . \ (-a)$ e, assim, $-(ba) \leq 0$. Aplicando agora o item (b), $-(-(ba)) \geq 0$ e, portanto, $ba \geq 0$.

Observe que a seção a respeito dos domínios de integridade não discutiu igualdade de duas instâncias dessa estrutura. Isso não foi feito, pelo fato de que a diferença entre um domínio (dependendo do contexto, pode-se omitir a expressão "de integridade") e um anel está apenas em uma propriedade adicional da multiplicação que não modifica estruturalmente a estrutura. Para anéis ordenados a coisa diferente: um anel ordenado é um anel "acrescido" de uma relação de ordem, de modo que temos de fazer menção a essa relação quando lhe fizermos referência (enquanto um anel é referido por $(A, +, .)$, um anel ordenado deve ser referido por $(A, +, ., \leq)$). Assim, é necessário incluir a relação de ordem no conceito de igualdade de anéis ordenados: dois anéis ordenados A e B são *isomorfos como anéis ordenados* (e serão considerados iguais) se existe um isomorfismo f de A em B tal que, para todos $a, b \in A$, $a \leq b$ implicar $f(a) \leq f(b)$.

3.7 Domínios bem ordenados

Falta pouco para a caracterização axiomática dos números inteiros. Para isso, há a necessidade de mais algumas definições a respeito de anéis ordenados.

Definição: um subconjunto S de um anel ordenado A é dito *limitado inferiormente* se $S = \varnothing$ ou se existir um elemento $a \in A$ tal que para todo $x \in S$ se tenha $x \geq a$.

Definição: diz-se que o subconjunto S de um anel ordenado tem *elemento mínimo* se existir $b \in S$ tal que para todo $x \in S$ se tenha $x \geq b$. (É fácil ver que se um subconjunto S tem um elemento mínimo, então ele é único. De fato, se b' e b'' são elementos mínimos de S, $b' \leq b''$ e $b'' \leq b'$ e então, pela antissimetria da relação de ordem, $b' = b''$).

Definição: um domínio de integridade ordenado A é dito *domínio bem ordenado* se satisfizer a seguinte propriedade.

Princípio da Boa Ordenação (PBO)

Todo subconjunto de A não vazio e limitado inferiormente possui elemento mínimo.

Será provado na seção seguinte que todos os domínios bem ordenados são isomorfos como anéis ordenados e, portanto, existe um

único domínio bem ordenado. Para isso necessitamos discutir uma propriedade importante de predicados definidos em domínios bem ordenados. Como veremos, essa propriedade se assemelha ao terceiro postulado de Peano e, por essa razão, também é chamado de *Princípio da Indução Matemática*. Para sua demonstração, precisamos de uma propriedade básica dos domínios bem ordenados, que estabelece que não existe elemento de um domínio ordenado entre os elementos neutros da adição e da multiplicação (0 e 1, para lembrar).

Proposição 7.3

Num domínio bem ordenado D, se $x > 0$, então $x \geq 1$.

Demonstração

Seja o conjunto $S = \{y \in D | 0 < y < 1\}$. Devemos mostrar que $S = \varnothing$. Por redução ao absurdo, suponhamos que $S \neq \varnothing$. Assim, pelo PBO S tem um elemento mínimo b. De $b < 1$ e $b > 0$, segue que (ver exercício 3.7) $b^2 < b$, o que implica, por transitividade, $b^2 < 1$. De $b > 0$ segue $b^2 > 0$. Assim, $b^2 \in S$. Porém, essa pertinência contraria o fato de que b é elemento mínimo de S, já que $b^2 < b$. Assim $S = \varnothing$ e a proposição está demonstrada.

É consequência imediata dessa propriedade o fato de que em um domínio bem ordenado não existe elemento entre dois elementos do tipo y e $y + 1$.

Corolário 1.3

Em um domínio bem ordenado D, se $x > y$, então $x \geq y + 1$.

Demonstração

De $x > y$ segue que $x - y > 0$ e então, pela proposição, $x - y \geq 1$. Daí, $x \geq y + 1$.

(Esse corolário justifica a denominação de *consecutivos* para elementos do tipo y e $y + 1$, sendo $y + 1$ o *consecutivo* de y, como definido na seção 2.2).

Teorema 1.3 (*Princípio da Indução Matemática*)

Sejam D um domínio bem ordenado, k um elemento de D e p um predicado no conjunto $A = \{z \in D | \, z \geq k\}$. Suponhamos que

(i) $p(k) = \text{V}$,

(ii) Para todo $z \geq k$, se $p(z) = \text{V}$, então $p(z + 1) = \text{V}$.

Então p é uma tautologia em A, isto é, $p(z) = \text{V}$ para todo $z \geq k$.

Demonstração

Basta provar que o conjunto $S = \{z \in D | \, z \geq k \text{ e } p(z) = \text{F}\}$ é vazio. Suponhamos, por redução ao absurdo, que $S \neq \varnothing$. Se assim fosse, como S é limitado inferiormente, pelo PBO, S teria um elemento mínimo b. Como pela hipótese (i), $k \notin S$, teríamos $b > k$ e então, pelo corolário 1.3, $b \geq k + 1$, o que implicaria $b - 1 \geq k$. Do fato

de que b é elemento mínimo de S e desta última desigualdade concluir-se- ia que $p(b - 1) = V$. Porém, a hipótese (ii) implicaria, a partir de $p(b - 1) = V$, que $p(b) = V$, o que contrariaria o fato de que $b \in S$. Logo $S = \varnothing$ e p é uma tautologia em A.

Como nos naturais, no Princípio da Indução Matemática a hipótese (i) é chamada *base da indução* e a assunção de que $p(z) = V$ é chamada *hipótese de indução* ou *hipótese indutiva*.

Observe que o Princípio da Indução Matemática oferece uma técnica bastante interessante de se provar assertivas matemáticas que são válidas para todos os elementos de um domínio bem ordenado maiores do que ou iguais a um certo elemento k. Basta verificar que a tal assertiva é verdadeira para o tal k e provar que se ela for verdadeira para um elemento $z > k$, sê-lo-á para o consecutivo z + 1. Assim como a afirmação era verdadeira para k, seria verdadeira para $k + 1$, seria verdadeira para $(k + 1) + 1$, e assim por diante, sendo verdadeira, portanto, para todo elemento do domínio bem ordenado maior do que ou igual a k.

3.8 O conjunto dos números inteiros

Mostraremos nesta seção que todos os domínios bem ordenados são isomorfos como anéis ordenados. Isso significa que

todos os domínios bem ordenados são iguais e, portanto, existe um único domínio bem ordenado. Este único domínio bem ordenado é chamado *conjunto dos números inteiros*, *anel dos inteiros* ou *domínio dos inteiros* e é representado por $\mathbb{Z}$, (da palavra alemã *zahl*, que significa número). Da própria denominação do conjunto, cada elemento de $\mathbb{Z}$ é chamado *número inteiro* ou simplesmente *inteiro*.

Sejam $(A, +, .)$ um anel, $(D, \#, *)$ um domínio bem ordenado, a um elemento de A e z um elemento de D. O *múltiplo* de *a por z* é o elemento de A, indicado por $z \times a$ (lido *z vez(es) a*), definido por

$$z \times a = \begin{cases} a + (z - 1) \times a, \text{se } z > 0_D \\ 0_A, \text{se } z = 0_D \\ -\big((\sim z) \times a\big), z < 0_D \end{cases}$$

onde ~ está indicando a subtração em D e – a subtração em A. Por exemplo,

$$1_D \times a = a + (1_D \sim 1_D) \times a = a + 0_D \times a = a + 0_A = a.$$

$$2_D \times a = a + (2_D \sim 1_D) \times a = a + 1_D \times a = a + a.$$

Proposição 8.3

Sejam $(A, +, .)$ um anel e $(D, \#, *)$ um domínio bem ordenado. Quaisquer que sejam $a, b \in A$ e $m, n \in D$, temos

a) $(\sim m) \times a = -(m \times a)$.

b) $(m \# n) \times a = (m \times a) + (n \times a)$.

c) $m \times (a + b) = (m \times a) + (m \times b)$.

d) $(m * n) \times a = m \times (n \times a)$.

e) $m \times (ab) = (m \times a)b$.

Demonstração

a) Se $m > 0_D$, $\sim m < 0_D$ e então $(\sim m) \times a = -((\sim(\sim m)) \times a) =$ $= -(m \times a)$ pois $\sim(\sim m) = m$. Se $m = 0_D$ a igualdade é evidente, pois ambos os seus termos ficam iguais a zero e se $m < 0_D$, da própria definição segue que $m \times a = -((\sim m) \times a)$ o que implica a igualdade pretendida.

b) Suponhamos que $m \# n > 0$, fixemos m e provemos a igualdade para todo $n \geq 1_D$. (para n negativo, fixaríamos n *e* faríamos a indução em relação a m que, forçosamente, seria positivo)

(i) É claro que a igualdade é verdadeira para $n = 1_D$, pois $(m \# 1_D) \times a = a + ((m \# 1 \sim 1) \times a) = a + (m \times a) = (m \times a) + a =$ $= (m \times a) + 1_D \times a$, onde a última igualdade decorre da igualdade $1_D \times a = a$ mostrada no exemplo acima.

(ii) Suponhamos que $(m \# n) \times a = (m \times a) + (n \times a)$ e provemos que $(m \# (n \# 1_D)) \times a = m \times a + ((n \# 1_D) \times a)$. Temos

$$(m \# (n \# 1_D)) \times a = a + ((m \# (n \# 1_D) \sim 1_D) \times a)$$

$$(m \# (n \# 1_D)) \times a = a + ((m \# n) \times a)$$

$$(m \# (n \# 1_D)) \times a = a + (m \times a) + (n \times a)$$

$$(m \# (n \# 1_D)) \times a = (m \times a) + (n \times a) + a$$

$$(m \# (n \# 1_D)) \times a = (m \times a) + ((n \# 1_D) \times a)$$

Se $m \# n < 0_D$, temos $(m \# n) \times a = -((\sim(m \# n)) \times a) =$ $= -((\sim m \sim n) \times a)$ o que implica $(m \# n) \times a = -(((\sim m) \times a) +$ $+ ((\sim n) \times a))$, já que $\sim m \sim n > 0_D$. Daí, $(m \# n) \times a = -((\sim m) \times a) -$ $- ((\sim n) \times a)) = -(-(m \times a) - (-(n \times a)) = m \times a + n \times a$, onde na penúltima igualdade foi utilizado o item (a) da proposição.

c) Provemos, por indução, que a igualdade é verdadeira para todo $m \geq 0_D$.

(i) Para $m = 0_D$ os dois termos da igualdade tornam-se iguais a zero e a igualdade é verdadeira.

(ii) Suponhamos que $m \times (a + b) = (m \times a) + (m \times b)$ e provemos que $(m \# 1_D) \times (a + b) = ((m \# 1_D) \times a) + ((m \# 1_D) \times b)$. Temos, para $m > 0_D$

$$(m \# 1_D) \times (a + b) = (m \times (a + b)) + (1_D \times (a + b))$$

$$(m \# 1_D) \times (a + b) = (m \times a) + (m \times b) + a + b$$

$$(m \# 1_D) \times (a + b) = ((m \# 1_D) \times a) + ((m \# 1_D) \times b)$$

e para $m < 0_D$,

$$m \times (a + b) = -((\sim m) \times (a + b))$$

$$m \times (a + b) = -(((-m) \times a) + ((-m) \times b))$$

$$m \times (a + b) = -((\sim m) \times a) + (-((-m) \times b)$$

$$m \times (a + b) = (m \times a) + (m \times b)$$

d) Como na demonstração do item (b), suponhamos que $m * n > 0$, fixemos m e provemos a igualdade para todo $n \geq 1$.

(i) É claro que a igualdade é verdadeira para $n = 1_D$, pois $(m * 1_D) \times a = m \times a = m \times (1_D \times a)$ por que mostramos no exemplo acima que $1_D \times a = a$.

(ii) Suponhamos que $(m * n) \times a = m \times (n \times a)$ e provemos que $(m * (n \# 1_D)) \times a = m \times ((n \# 1_D) \times a)$. Temos

$$(m * (n \# 1_D)) \times a = ((m * n) \# m) \times a$$

$$(m * (n \# 1_D)) \times a = ((m * n) \times a) + (m \times a)$$

$$(m * (n \# 1_D)) \times a = m \times (n \times a) + (m \times a)$$

$$(m * (n \# 1_D)) \times a = m \times ((n \times a) + a)$$

$$(m * (n \# 1_D)) \times a = m \times ((n \# 1_D) \times a)$$

Se $m * n = 0_D$, temos $m = 0_D$ ou $n = 0_D$ (D é um domínio) e os dois termos da igualdade são iguais a zero. Se $m * n < 0_D$,

$$(m * n) \times a = -((\sim(m * n)) \times a)$$

$$(m * n) \times a = -(((\sim m) * n) \times a)$$

$$(m * n) \times a = -((\sim m) \times (n \times a))$$

$$(m * n) \times a = -(- (m \times (n \times a)))$$

$$(m * n) \times a = m \times (n \times a)$$

e) Provemos que a igualdade é verdadeira para $m \geq 0_D$.

(i) A igualdade é claramente verdadeira para $m = 0_D$, pois

ambos os termos se tornam iguais a zero.

(ii) Suponhamos que $m \times (ab) = (m \times a)b$ e provemos que $(m \# 1_D) \times (ab) = ((m \# 1_D) \times a)b$. Temos

$$(m + 1_D) \times (ab) = m \times (ab) + ab$$

$$(m + 1_D) \times (ab) = (m \times a)b + ab$$

$$(m + 1_D) \times (ab) = (m \times a + a)b$$

$$(m + 1_D) \times (ab) = ((m \# 1_D) \times a)b$$

Para $m < 0$, $m \times (ab) = -((\sim m) \times (ab)) = -(((\sim m) \times a)b) =$ $= (m \times a)b$.

Corolário 2.3

Nas condições da proposição anterior, $(m * n) \times (ab) = (m \times a)(n \times b)$.

Demonstração

Temos $(m * n) \times (ab) = m \times (n \times (ab)) = (m \times (n \times a))b =$ $= m \times ((n \times a)b) = m \times (n \times (ab)) = m \times (n \times (ba)) = m \times ((n \times b)a) =$ $= m \times (a\ (n \times b)) = (m \times a)(n \times \mathrm{b})$.

Corolário 3.3

Se A é um anel ordenado, D é um domínio bem ordenado e um elemento m de D é tal que $m > 0_D$, então $m \times 1_A > 0_A$.

Demonstração

Por indução, para $m = 1_D$ temos que $1_D \times 1_A = 1_A > 0$, conforme

o exercício 3.6. Suponhamos que $m \times 1_A > 0_A$ e provemos que $(m \# 1_D) \times 1_A > 0_A$. Temos $(m \# 1_D) \times 1_A = m \times 1_A + 1_D \times 1_A > 0$, pois ambas as parcelas são maiores que zero, a primeira pela hipótese de indução e a segunda pela base de indução.

Teorema 2.3

Se $(D, +, .)$ e $(E, \#, *)$ são domínios bem ordenados, então a função ρ de E em D definida por $\rho(z) = z \times 1_D$ é um isomorfismo de anéis ordenados.

Demonstração

Inicialmente, temos

i) $\rho(z_1 \# z_2) = (z_1 \# z_2) \times 1_D = (z_1 \times 1_D) + (z_2 \times 1_D) =$
$= \rho(z_1) + \rho(z_2)$.

ii) $\rho(z_1 * z_2) = (z_1 * z_2) \times 1_D = (z_1 \times 1_D)(z_1 \times 1_D) =$
$= (z_1)\rho(z_2)$, onde na segunda igualdade foi utilizado o corolário 2.3.

iii) $\rho(1_E) = 1_E \times 1_D = 1_D$,

Provemos agora ρ é sobrejetiva. Para tal devemos provar que todo elemento $a \in D$ é da forma $z \times 1_D$ para algum $z \in E$. Por contradição, suponhamos que existe $a \in D$ tal que $a \neq z \times 1_D$, para todo $z \in$ E e consideremos os conjuntos $A' = \{z \times 1_D \in D | \ z \in E$ e

$z \times 1_D > a\}$ e A" $= \{z \times 1_D \in D | \, z \in E$ e $z \times 1_D < a\}$.

Se $A' \neq \varnothing$, como ele é um conjunto limitado inferiormente e D é um domínio bem ordenado, pelo Princípio da Boa Ordenação, A' tem um elemento mínimo $b \times 1_D$. Assim, $b \times 1_D > a$ e $b \times 1_D - 1_D \leq a$. Desta última, segue $(b - 1_D) \times 1_D \leq a$, de que resulta $(b - 1_D) \times 1_D < a$, pois $a \neq z \times 1_D$, para todo $z \in E$. Desta desigualdade e do corolário 3.1 segue que $a \geq (b - 1_D) \times 1_D + 1_D = b \times 1_D$, o que contradiz a desigualdade $b(1_D) > a$. Logo $A' = \varnothing$. Utilizando raciocínio semelhante e a formulação do Princípio da Boa Ordenação dada no exercício 3.11, prova-se que A" também é um conjunto vazio, o que prova que não existe $a \in D$ tal que $a \neq z \times 1_D$, para todo $z \in E$. Logo, ρ é sobrejetiva.

Para provar que ρ é injetiva (e também que "preserva" as ordens dos domínios bem ordenados), sejam $z, y \in E$, com $z > y$. Daí, $z - y > 0$ e, como $\rho(z) - \rho(y) = z \times 1_D - y \times 1_D = (z - y) \times 1_D$, temos $\rho(z) > \rho(y)$. Assim, ρ é um isomorfismo de anéis ordenados e todos os domínios bem ordenados são iguais implicando a existência de um único domínio bem ordenado que, como foi dito no início da seção, é chamado *conjunto dos números inteiros*.

Sendo o único domínio bem ordenado, o domínio dos números inteiros (representado por $\mathbb{Z}$ como estabelecido no início da seção)

fica perfeitamente caracterizado: nele estão definidas duas operações que gozam das propriedades (A_1), (A_2), (A_3), (A_4), (M_1) (M_2), (M_3), (M_4) e (MA), nele está definida uma relação de ordem $\leq$ que é compatível com a adição e com a multiplicação e ele satisfaz ao Princípio da Boa Ordenação: todo subconjunto não vazio limitado inferiormente te um elemento mínimo. Além disso, o conjunto dos números inteiros satisfaz todas as propriedades fixadas neste capítulo (inclusive, para destacar, o Princípio da Indução Matemática). Nas seções e nos capítulos seguintes, será mostrado que todos os fatos conhecidos sobre os inteiros podem ser demonstrados a partir dessa caracterização.

3.9 Inversibilidade no domínio dos inteiros

O objetivo desta seção é mostrar que os únicos elementos inversíveis do domínio dos inteiros são 1 e -1. Para tal, necessitamos da seguinte definição. O *valor absoluto* ou *módulo* de um inteiro z é definido por $|z| = \begin{cases} z, \text{se } z \geq 0 \\ -z, \text{se } z < 0 \end{cases}$

Por exemplo, |1| = 1, |0| = 0 e |-1| = 1.

Observe que a definição $|z| = -z$ se $z < 0$ pode ser substituída por $|z| = -z$ se $z \leq 0$, pois o caso $z = 0$ implicaria em ambas $|z| = 0$, não

havendo dubiedades.

O *valor absoluto* satisfaz às propriedades listadas na seguinte proposição e nos seus corolários.

Proposição 9.3

Sejam $z, y \in \mathbb{Z}$. Então

a) $|z| \geq 0$ e $|z| = 0$ se e somente se $z = 0$.

b) $|zy| = |z||y|$.

c) $-|z| \leq z \leq |z|$.

d) $|z| < y$ se e somente se $-y < z < y$.

Demonstração

a) Decorre imediatamente da definição, pois se $z > 0$, $|z| = z > 0$ e se $z < 0$, $|z| = -z$ e $-z > 0$.

b) A demonstração dessa igualdade pode ser feita analisando-se os quatro casos possíveis de combinações de positividade e negatividade de y e de z:

(i) se $z \geq 0$ e $y \geq 0$, temos, pela compatibilidade da relação de ordem com a multiplicação, que $zy \geq 0$ e a igualdade a ser provada decorre da definição.

(ii) se $z \geq 0$ e $y \leq 0$, temos, pela proposição 6.3, $zy \leq 0$ e então

$|zy| = -(zy)$ (definição de valor absoluto)

$|zy| = z(-y)$ (item (b) da proposição 2.3)

$|zy| = |z||y|$ (definição de valor absoluto)

(iii) se $z \leq 0$ e $y \geq 0$ a demonstração é semelhante à anterior, já que, também neste caso, $zy \leq 0$.

(iv) finalmente, se $z \leq 0$ e $y \leq 0$, temos $zy \geq 0$ e $|zy| = zy = (-z)(-y) = |z||y|$.

c) Se $z \geq 0$, então $|z| = z \geq -|z|$, pois $-|z|$ é sempre negativo. Daí, $|z| \geq z \geq -|z|$. Se $z \leq 0$, então $|z| = -z$, $-|z| = z \leq |z|$, pois $|z|$ é sempre positivo e estamos na hipótese de que z é negativo. Segue então a afirmação.

d) Suponhamos inicialmente que $|z| < y$. Assim $-y < -|z|$ e então $-y < -|z| \leq z \leq |z| < y$, onde nas segunda e terceira desigualdades foi utilizado o item (c) anterior.

Reciprocamente, suponhamos que $-y < z < y$. Se $z \geq 0$, então $|z| = z$ e, assim, $|z| < y$. Se $z \leq 0$, temos $|z| = -z$ e, então, $|z| < y$, pois da hipótese $-y < z$ segue que $-z < y$.

Corolário 4.3

Sejam $z, y \in \mathbb{Z}$. Se $y \neq 0$, então $|zy| \geq |z|$.

Demonstração

Como $y \neq 0$ temos que $|y| > 0$ e então, pela proposição 7.3, $|y| \geq 1$. Daí, aplicando a compatibilidade com a multiplicação, tem-se $|z||y| \geq |z|1$ que implica a desigualdade procurada.

O corolário a seguir estabelece uma propriedade, chamada *propriedade arquimediana*, que será utilizada em demonstrações futuras.

Corolário 5.3 (*propriedade arquimediana)*

Se $z, y \in \mathbb{Z}$ e $y \neq 0$, então existe $n \in \mathbb{Z}$ tal que $ny \geq z$.

Demonstração

Pelo corolário anterior temos $|zy| \geq |z|$ e então $|y||z| \geq |z|$ que implica $|y||z| \geq z$, já que $|z| \geq z$. Daí, se $y > 0$, a desigualdade a ser demonstrada segue tomando $n = |z|$ e se $y < 0$ a desigualdade segue tomando $n = -|z|$.

Proposição 10.3

Os únicos inteiros inversíveis são 1 e -1.

Demonstração

Se $z \in \mathbb{Z}$ é inversível, então $z \neq 0$ e existe $y \in \mathbb{Z}$, $y \neq 0$, tal que $zy = 1$. De $z \neq 0$ segue que $|z| > 0$ que implica $|z| \geq 1$. Por outro lado, de $y \neq 0$ e do corolário 4.3, temos que $|zy| \geq |z|$ e, portanto, $|z| \leq 1$, pois $|zy| = 1$. Desta desigualdade e de $|z| \geq 1$ segue que $|z| = 1$ e, então, $z = 1$ ou $z = -1$.

3.10 Sequências estritamente decrescentes de inteiros

Nos capítulos 6 e 7, vamos necessitar de uma outra propriedade básica dos inteiros e para tal precisamos da seguinte definição. Uma *sequência* (ou *sucessão*) de elementos de um conjunto A é uma função do conjunto dos números naturais em A. Uma sequência f de elementos de um conjunto A é indicada por $(x_n) = (x_1, x_2, x_3, ..., x_n, ...)$, onde $x_n = f(n)$. (Na Matemática da educação básica, $x_n = f(n)$ é chamado *termo geral* da sequência). Em um anel ordenado, uma sequência (x_n) é dita *estritamente decrescente* se $x_1 > x_2 > x_3 > ... > x_n > ...$

Proposição 11.3

Não existe sequência estritamente decrescente de inteiros positivos.

Demonstração

Se existisse uma sequência (x_n) tal que $x_1 > x_2 > ... > x_n > ... > 0$, o conjunto $S = \{x \in D | x > 0\}$, não vazio e limitado inferiormente, não teria elemento mínimo, contrariando o PBO.

Corolário 6.3

Seja $k \in \mathbb{Z}$, com $k \geq 0$. Se os inteiros $x_1, x_2, x_3, \ldots, x_j, ...$ são

tais que $x_1 > x_2 > x_3 > ... > x_j > ... \geq k$, então existe n tal que $x_n = k$.

Demonstração

A não existência de n tal que $x_n = k$ implicaria que a sequência $x_1 - k > x_2 - k > ... > x_k - k > ... > 0$ contradiria a proposição.

3.11 Os naturais e os inteiros

Consideremos o conjunto $\mathbb{Z}_+ = \{z \in \mathbb{Z} | z > 0\}$ e a função f, de $\mathbb{Z}_+$ em $\mathbb{Z}_+$, definida por $f(z) = z + 1$. Observe que a desigualdade $z + 1 > z$ garante que f está bem definida e a aplicação da lei do corte dada na proposição 5.3 demonstra que f é injetiva. Além disso, da própria definição de f segue que $f(\mathbb{Z}_+) = \mathbb{Z}_+ - \{1\}$. Portanto $\mathbb{Z}_+$ satisfaz aos primeiro e segundo postulados de Peano. Além disso, o Princípio da Indução Matemática, dado no teorema 1.3, mostra que $\mathbb{Z}_+$ satisfaz também ao terceiro postulado de Peano. Ainda mais: (i) como são associativas e comutativas e a multiplicação é distributiva em relação à adição, as operações em $\mathbb{Z}_+$ coincidem com as operações em $\mathbb{N}$; (ii) se $y, z \in \mathbb{Z}_+$ e $y < z$ temos $z - y > 0$ e $y + (z - y) = z$ e as relações de ordem em $\mathbb{Z}_+$ e em $\mathbb{N}$ coincidem. Logo, $\mathbb{N} = \mathbb{Z}_+$. Observe que desta igualdade também podemos concluir que o conjunto dos inteiros é um conjunto infinito.

3.12 Exercícios

Para receber propostas de soluções, basta enviar e-mail para jaime@ic.ufal.br com as seguintes informações: nome completo, categoria (discente/docente), curso, instituição, estado/cidade.

3.1 Construa um anel (A, +, .), em que A é um conjunto finito de cardinalidade mínima.

3.2 Sejam A um anel e $a, b, c \in A$. Mostre que

a) Se $a + c = b + c$, então $a = b$.

b) Se $a + b = a$ para algum $a \in A$, então $b = 0$.

c) $-(a + b) = -a - b$.

d) $a^2 - b^2 = (a + b).(a - b)$

3.3 Mostre que o produto de dois elementos de um anel é inversível se e somente se os dois elementos são inversíveis.

3.4 Sejam $(A, +, \cdot)$ um anel e A' um subconjunto de A. O subconjunto A' é dito um *subanel de A* se $(A', +_{A'}, \cdot_{A'})$ é um anel tal que $1_{A'} = 1_A$ (naturalmente, as operações $+_{A'}$ e $\cdot_{A'}$ são as restrições de + e de . ao conjunto A'xA').

a) Sejam A um anel e A' um subconjunto de A. Mostre que A' é um subanel de A se e somente se

i) $1_A \in A'$.

ii) $a - b \in A'$ e $ab \in A'$, $\forall a, b \in A'$

b) Sejam A e B dois anéis e f um homomorfismo de A em B ($f : A \to B$ tal que $f(a + b) = f(a) \# f(b)$, $f(a \,.\, b) = f(a) * f(b)$ e $f(1_A) = 1_B$). Mostre que $f(A)$ é um subanel de B.

3.5. Alguns autores não incluem a comutatividade da multiplicação como axioma para a construção de um anel. Para estes, quando a comutatividade existe, o anel é dito *comutativo* ou *booleano*. Para aqueles que incluem a comutatividade da multiplicação como axioma, um conjunto munido de duas operações que gozem das propriedades (A_1), (A_2), (A_3), (A_4), (M_1), $(M_3,)$, (M_4) e (AM) é um *anel não comutativo*. Seja A um anel e $\mathfrak{I}(A)$ o conjunto das funções de A em A. Dadas f e g em $\mathfrak{I}(A)$, defina a adição $f + g$ pela função dada por $(f + g)(x) = f(x) + g(x)$. Verifique se $\mathfrak{I}(A)$ munido dessa adição e da composição de funções é um anel não comutativo.

3.6. Seja D um domínio de integridade. Mostre que

a) Se $a^2 = 0$, então $a = 0$.

b) Se $ab = a$ então $a = 0$ ou $b = 1$.

c) Se $a^2 = a$, então $a = 0$ ou $a = 1$.

3.7. Sejam A um anel e $a \in A$, com $a \neq 0$. Considere a função $f_a : A \to A$, definida por $f_a(x) = ax$.

a) Mostre que f_a é sobrejetora se e somente se a é

inversível.

b) Mostre que se A é um domínio de integridade, então f_a é injetora.

3.8 Sejam A um anel ordenado e $a, b, c, d \in A$. Mostre que

a) Se $a + c \leq b + c$, então $a \leq b$.

b) Se $a \leq b$ e $c \leq d$, então $a + c \leq b + d$.

c) Se $a \leq b$ e $c \leq 0$, então $ac \geq bc$.

d) Se $a < b$ e $b < c$, então $a < c$.

e) Se $a < b$ e $b \leq c$, então $a < c$.

f) Se $a < b$, então $a + k < b + k$, para todo $k \in A$.

g) Se $a < b$ e $c < d$, então $a + c < b + d$.

h) Se $a \leq b$ e $c < d$, então $a + c < b + d$.

3.9. Seja A um anel ordenado. Mostre que

a) $a^2 \geq 0$, qualquer que seja $a \in A$.

b) $1 > 0$.

c) $-1 < 0$.

d) Qualquer que seja $a \in A$, $a < a + 1$.

3.10. Mostre que não se pode munir o anel I_{12} de uma relação de ordem que o transforme num anel ordenado.

3.11. Sejam A um domínio de integridade ordenado e $a, b, c \in A$. Mostre que

a) Se $a < b$ e $c > 0$, então $ac < bc$.

b) Se $ac \leq bc$ e $c > 0$, então $a \leq b$.

c) Se $ac \leq bc$ e $c < 0$, então $a \geq b$.

3.12. Sejam A um anel ordenado e S um subconjunto de A. Diz-se que S é *limitado superiormente* se existir $a \in A$ tal que $x \leq a$, qualquer que seja $x \in S$. Diz-se que S tem *elemento máximo* se existir $b \in S$ tal que $x \leq b$, qualquer que seja $x \in S$. Mostre que

a) Se S tem elemento máximo, então este elemento é único.

b) O Princípio da Boa Ordenação é equivalente à seguinte propriedade.

Todo subconjunto não vazio limitado superiormente possui elemento máximo.

3.13. Como fixamos anteriormente, $2 = 1 + 1$ e, portanto, $2 \neq 1$. Entretanto, pode-se "provar" que $2 = 1$ da seguinte forma.

Sejam a e b dois inteiros tais que $a = b$. Multiplicando ambos os termos por a temos $a^2 = ab$, donde se conclui (somando a ambos os termos $a^2 - 2ab$) a igualdade $a^2 + a^2 - 2ab = a^2 - 2ab + ab$. Daí, $2a^2 - 2ab = a^2 - ab$ e, então, $2(a^2 - ab) = 1(a^2 - ab)$ que dá, pela lei do cancelamento, $2 = 1$.

Evidentemente, essa "demonstração" está errada! Determine

qual o erro cometido.

3.14. Seja $z \in \mathbb{Z}$. Mostre que se $z < 0$, então $z \leq -1$.

3.15. Sejam $z, y \in \mathbb{Z}$**.** Mostre que

a) $|z + y| \leq |z| + |y|$ (*desigualdade triangular*).

b) $||z| - |y|| \leq |z + y| \leq |z| + |y|$.

c) $||z| - |y|| \leq |z - y| \leq |z| + |y|$.

3.16. Dados $z, n \in \mathbb{Z}$, $z \neq 0$ e $n \geq 0$, definimos *potência de base z e expoente n* por $z^n = \begin{cases} 1, \text{se } n = 0 \\ z \,.\, z^{n-1}, n > 0 \end{cases}$ (z^n também é lido *z elevado a n*)

Mostre que para todos $a, b, m, n \in \mathbb{Z}$, com $a, b \neq 0$ e $m, n \geq 0$ temos

a) $a^m b^m = (ab)^m$.

b) $a^m a^n = a^{m+n}$.

c) $(a^m)^n = a^{m.\,n}$.

3.17. Sejam a e b dois inteiros. Mostre que

a) se $a < b$, então $a^3 < b^3$.

b) $a^2 - ab + b^2 \geq 0$.

c) se $a > 1$ e m e n são dois inteiros positivos, então $a^m > a^n$ se e somente se $m > n$.

3.18. Mostre que qualquer que seja o inteiro $k \geq 3$ se tem $2k + 1 < 2^k$.

3.19. Mostre que qualquer que seja o inteiro $k \geq 5$ se tem $k^2 < 2^k$.

3.20. Seja $\frac{z}{2}$ o número inteiro y (se existir) tal que $2y = z$. Considerando as condições de existência, mostre que, $\frac{z}{2} + w = \frac{z + 2w}{2}$.

3.21. Sejam x_1 e r dois números inteiros. A *Progressão Aritmética* (PA) de *primeiro termo* x_1 e *razão* r é a sequência de números inteiros $(x_1, x_2, x_3, \ldots)$ tal que $x_{k+1} = x_k + r$, qualquer que seja o valor de $k = 1, 2, 3, \ldots$ Mostre que se $(x_1, x_2, x_3, \ldots, x_n, ...)$ é uma PA de razão r, então:

a) $x_n = x_1 + (n - 1)r$.

b) Se $S_n = x_1 + x_2 + \ldots + x_n$, então $S_n = \frac{(x_1 + x_n)n}{2}$. (Na educação básica, S_n é chamada *soma dos termos da PA*)

3.22. Sejam x_1 e q dois números inteiros não nulos. A *Progressão Geométrica* (PG) de *primeiro termo* x_1 e *razão* q é a sequência de números inteiros $(x_1, x_2, x_3, \ldots)$ tal que $x_{k+1} = x_k q$, qualquer que seja o valor de $k = 1, 2, 3, \ldots$ Mostre que se $(x_1, x_2, x_3, \ldots, x_n, ...)$ é uma PG de razão r, então:

a) $x_n = x_1 q^{(n-1)}$.

b) Se $S_n = x_1 + x_2 + \ldots + x_n$, então $S_n = \frac{x_1(q^n - 1)}{q - 1}$. (Na Educação Básica, S_n é chamada *soma dos termos da PG*)

3.23. Sejam a, b e n números inteiros, com $n > 1$. Mostre que $a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \ldots + ab^{n-2} + b^{n-1})$.

3.24. Dado $n \in \mathbb{Z}$, $n \geq 0$, definimos o *fatorial de n* por

$$n! = \begin{cases} 1, \text{se } n = 0 \text{ ou } n = 1 \\ n(n-1)!, \text{se } n > 1. \end{cases}$$

Mostre que se A e B são dois conjuntos finitos não vazios e $|A| = |B| = n$, então o número de bijeções de A em B é $n!$.

3.25. Seja um inteiro z tal que $z \geq -1$. Mostre que se n é um inteiro positivo, então $(1 + z)^n \geq 1 + nz$, desigualdade conhecida como *Desigualdade de Bernoulli*.

3.26. O jogo conhecido como *Torre de Hanói* consiste de n discos de diâmetros diferentes, perfurados, e dispostos em uma haste vertical *origem* na ordem decrescente dos seus diâmetros. O objetivo do jogo é mover todos os discos da haste *origem* para uma outra haste *destino*, utilizando uma terceira haste *auxiliar*, devendo-se mover um disco de cada vez e não sendo permitir dispor um disco sobre outro de diâmetro maior. Por exemplo, se $n = 1$, basta se deslocar esse disco da *origem* para o *destino*; se $n = 2$, os movimentos seriam:

origem $\rightarrow$ *auxiliar*

origem $\rightarrow$ *destino*

auxiliar $\rightarrow$ *destino*.

Mostre que se a_n é o número mínimo de movimentos para se

concluir a Torre de Hanói, então

a) $a_n = 2a_{n-1} + 1$, para $n \geq 2$.

b) $a_n = 2^n - 1$, para todo inteiro $n \geq 1$.

3.27. Seja A um conjunto finito, com $|A| = n$. Mostre que $|\wp(A)| = 2^n$.

3.28. Seja $\mathbb{Z}^* = \{z \in \mathbb{Z} | z \neq 0\}$ e defina em $\mathbb{Z}x\mathbb{Z}^*$ a relação $(a, b) \approx (c, d)$ se $ad = bc$. Mostre que $\approx$ é uma relação de equivalência.

3.29. Mostre que a operação $(a, b) \# (c, d) = (ac - bd, ad + bc)$ definida no conjunto $\mathbb{Z}x\mathbb{Z}^*$ da questão anterior tem elemento neutro.

4. Algoritmos

4.1 Introdução

Tendo definido axiomaticamente os inteiros e obtido algumas de suas propriedades básicas, apresentaremos no próximo capítulo formas de representá-los. Para tal necessitaremos demonstrar algumas outras propriedades desses números, dentre elas a existência de inteiros que gozam de uma propriedade específica. Neste capítulo, discutiremos uma técnica utilizada em demonstrações de existência de objetos matemáticos que satisfazem determinada propriedade. A ideia é a seguinte: para se provar que existe um inteiro que satisfaça uma propriedade específica apresenta-se uma "receita" de como encontrar tal inteiro. Em Matemática e Ciência da Computação, uma "receita" com esse ou qualquer outro objetivo é chamada de *algoritmo*.

A definição formal de algoritmo é desenvolvida no campo da *Teoria da Computação* e envolve conceitos que não estão no escopo deste livro. Aqui, consideraremos informalmente um algoritmo como uma *sequência de instruções,* que podem ser executadas por uma máquina ou por um ser humano, de tal forma que ao final da execução uma tarefa tenha sido realizada, exatamente aquela tarefa para a qual

o algoritmo foi desenvolvido.

No dia a dia, uma receita de bolo, o roteiro para instalação ou para utilização de um equipamento eletrônico são algoritmos. Uma partitura musical também é um algoritmo. Uma receita de bolo começa com a *relação dos ingredientes* e continua com instruções do tipo *misture*, *aqueça*, *bata as claras até o ponto de neve*, etc. Um roteiro para instalação de um equipamento eletrônico começa - embora isto fique implícito - com o próprio *equipamento eletrônico*, com *cabos*, *conectores*, *antenas*, etc. e continua com instruções do tipo *ligue o cabo X ao conector A*, *se for usar antena externa ligue o cabo Z ao conector B*, etc. Os ingredientes de uma receita de bolo e um equipamento eletrônico, os cabos e os conectores no roteiro para instalação do tal equipamento são as *entradas* dos algoritmos correspondentes. Aparecem em seguida as instruções e finalmente tem-se a *saída* do algoritmo que, nestes dois exemplos, são o bolo pronto e o equipamento instalado. Isto significa que, de um modo geral, o desenvolvimento de um algoritmo requer que seja fixada sua *entrada* e sua *saída*, que é, exatamente, a realização da tarefa para a qual o algoritmo foi desenvolvido. O algoritmo propriamente dito é constituído do conjunto de instruções que executadas sobre a *entrada* fornece a *saída* esperada.

Naturalmente, como a linguagem da ciência deve ser precisa,

as instruções de um algoritmo devem satisfazer algumas condições:

1. Uma instrução não pode conter nenhum tipo de ambiguidade que permita que sua execução dependa de algum tipo de "subjetividade" do executor.

2. Após a execução de uma instrução, não deve haver ambiguidade relativa a qual instrução será executa a seguir.

3. Toda instrução deve ser executada em um intervalo de tempo finito (no sentido usual da expressão), o que significa que a execução do algoritmo deve *parar* em algum momento.

Se, além do exigido acima, exigirmos que as instruções de um algoritmo sejam executadas sequencialmente, sempre na ordem em que elas estão escritas, uma instrução tendo sua execução iniciada somente após a conclusão da execução da instrução anterior, o algoritmo será dito *estruturado*. É dessa forma que os algoritmos serão aqui apresentados e, assim, suporemos sempre que ao final da execução da última instrução a execução do algoritmo estará encerrada.

As entradas dos nossos algoritmos, números basicamente, serão "armazenadas" em *variáveis* que são representadas por letras ou nomes sugestivos em relação ao seu objetivo (no capítulo 6, utilizaremos variáveis "indexadas"). A instrução que indicará que haverá uma entrada e que esta será armazenada na variável x será

escrita *leia*(*x*)*;* e é chamada *comando de entrada*. A saída do algoritmo será dada através do comando *escreva(x*/*mensagem);* que exibirá o *conteúdo* da variável *x* ou a *mensagem* pretendida (quando se tratar de uma mensagem, ela será colocada entre apóstrofos).

Variáveis também serão utilizadas para armazenar valores durante a execução do algoritmo. Para isso, utilizaremos a instrução *variável* := *valor;*. Por exemplo, uma instrução *x* := 1*;* significa que, a partir da execução desta instrução, o conteúdo da variável *x* é 1. Uma instrução deste tipo é chamada *comando de atribuição* e o segundo membro pode conter expressões aritméticas. Por exemplo, ao final da execução da sequência de instruções

x := 1;
y := 1;
w := *x* + *y*;
y := *y* - *w*;

em *x* estará armazenado 1, em *w*, o valor 2, e em *y*, -1.

Outra instrução que consideraremos, chamada *comando de decisão*, é a instrução

se p
  então execute estas instruções
  senão execute estas instruções;

onde *p* é um predicado no *universo* do problema que se está tratando. É fácil perceber que a execução de um comando de decisão seleciona, dependendo do valor do predicado *p*, a sequência de instruções que

será executada. A opção *senão* é facultativa e quando ela não aparece e o predicado é falso nada é executado e passa-se à execução da instrução seguinte.

Finalmente, necessitaremos de instruções que permitam a repetição da execução de uma sequência de instruções. Estas instruções são chamadas *comandos de repetição* e utilizaremos dois tipos com objetivos autoexplicativos:

1) *repita N vezes*
    sequência de instruções

2) *repita enquanto p*
    sequência de instruções

Nesse segundo tipo, p é um predicado e a sequência de instruções será executada enquanto o valor de p for V.

Nos comandos de seleção e de repetição a utilização de tabulações distintas indicará qual a sequência de instruções que está vinculada àquele comando. Nos comandos de repetição, cada execução da sequência de instruções é chamada *iteração* ou *laço*.

Apresentaremos a seguir alguns exemplos de algoritmos. Para ser possível a compreensão de alguns destes exemplos, vamos considerar conhecidos o conjunto dos números reais e as operações neste conjunto.

4.2 Exemplos

1. Considerando conhecido o conceito de *média aritmética*, o algoritmo abaixo recebe como entrada três números e fornece como saída a média aritmética de três números.

```
algoritmo Média de três números;
   leia(x, y, z);
   Media := (x + y + z)/3;
   escreva(Media);
```

2. Naturalmente, a extensão do algoritmo anterior para o cálculo da média de muitos números (cinco mil, por exemplo), seria impraticável (imagine como ficariam as primeira e segunda instruções!). A solução seria utilizar uma única variável *x* para receber todos os números, só recebendo um próximo quando o anterior já estivesse sido processado (somado com os anteriores). Para isso utiliza-se uma outra variável que vai armazenado as somas parciais, recebendo essa variável o valor inicial zero, para que o primeiro número possa ser somado.

```
algoritmo Média de n números;
   leia(n);
   Soma := 0;
   repita n vezes
      leia(x);
      Soma := Soma + x;
   Media := Soma/n;
```

```
escreva(Media);
```

3. O algoritmo abaixo calcula a *potência* a^n, a e n dados, definição dada em um dos exercícios do capítulo 3.

```
algoritmo Potência;
   leia(a, n);
   Potencia := 1;
   se n > 0
      então
         repita n vezes
            Potencia := potência . a;
   escreva(Potencia);
```

Observe que se o expoente é zero ($n = 0$) o comando de repetição não é executado e a saída da potência é 1, de acordo com a definição (o algoritmo não "está preparado" para valores negativos de n). Observe também que o número de iterações deste algoritmo é n. Isto significa que o número de multiplicações necessária para se calcular a^n é n. Naturalmente o número de operações necessárias para a execução de um algoritmo é uma medida de sua *eficiência*. No capítulo seguinte, discutiremos um algoritmo mais eficiente para o cálculo de potências.

4. O algoritmo abaixo retorna o *fatorial de um número inteiro positivo* dado, conforme definido em um exercício do capítulo 3.

```
algoritmo Fatorial;
   leia(n);
   Fatorial := 1;
```

```
se n < 0
   então
         escreva('Não existe fatorial de número negativo')
   senão
         se n > 1
            então
               i := 2;
               repita enquanto i ≤ n
                  Fatorial := Fatorial . i;
                  i := i + 1;
               escreva(fatorial);
```

5. O exemplo que vamos discutir agora foge um pouco da matemática, mas é importante para a compreensão de algoritmos. Imagine que queremos receber dois números e armazená-los em ordem crescente em duas variáveis x e y fixadas. Isto significa que queremos "receber" os dois números em qualquer ordem e pretendemos que ao final da execução do algoritmo o menor deles esteja armazenado na variável x e outro na variável y. Naturalmente, a ordem em que aparecem no algoritmo os comandos *leia*(x); e *leia*(y); indicará o armazenamento dos números fornecidos. Se a ordem for essa e o menor dos números for digitado inicialmente, nada precisa ser feito; se isso não acontecer devemos trocar os conteúdos de x e de y.

```
algoritmo Ordena dois números
   leia(x);
   leia(y);
   se x > y
```

```
    então
        Aux := x;
        x := y;
        y := Aux;
  escreva(x, y);
```

6. O nosso último de exemplo de "algoritmo" é uma sequência de instruções que não se sabe ainda se ela constitui um algoritmo. Como foi dito, uma condição para que uma sequência de instruções seja um algoritmo é que sua execução pare, retornando uma saída, qualquer que seja a entrada compatível. (A definição de inteiro *ímpar* encontra-se no exercício 5.7).

algoritmo (?) de Collatz
 leia(z);
 repita enquanto z > 1
    se z é ímpar
       então
          z := 3z + 1;
       senão
          z := $\frac{z}{2}$;
       escreva(z);

Este é um dos problemas de Matemática que ainda não tem solução, embora todos os matemáticos concordem que, de fato, se trata de um algoritmo. Tomás Oliveira e Silva, da Universidade de Aveiro, Portugal, executou (em um computador, é claro) esse algoritmo para todos os inteiros menores que $19 \cdot 2^{55}$ e não encontrou

nenhum contraexemplo. (No próximo capítulo, veremos o significado de 19 e de 55, desculpem o exagero).

4.3 Exercícios

Para receber propostas de soluções, basta enviar e-mail para jaime@ic.ufal.br com as seguintes informações: nome completo, categoria (discente/docente), curso, instituição, estado/cidade.

4.1. O algoritmo *Ordena dois números* acima possui uma sequência de comandos que troca o conteúdo de duas variáveis x e y. Para tal era utilizada uma variável *Aux* como variável auxiliar, que armazenava temporariamente o conteúdo de x, para que este não fosse "perdido" quando x recebesse o conteúdo de y. Escreva uma sequência de comandos de atribuição que, sem utilizar uma terceira variável, realiza a troca de conteúdos de duas variáveis.

4.2. Escreva um algoritmo que ordena três números dados.

4.3. Um inteiro positivo z é dito *quadrado perfeito* se existe um inteiro x tal que $x^2 = z$, caso em que x é chamado *raiz quadrada* de z, indicado por $\sqrt{z}$. Por exemplo, $\sqrt{9} = 3$. Escreva um algoritmo que verifica se um inteiro dado é um quadrado perfeito e retorna sua raiz quadrada.

4.4 Escreva um algoritmo que forneça o maior de três números dados.

5. Representação dos números inteiros: sistemas de numeração

5.1 Introdução

Já sabemos que o conjunto dos inteiros é um conjunto infinito, mas só sabemos representar alguns deles: 0, 1, 2, ...12 e seus respectivos simétricos. Neste capítulo aprenderemos como representar inteiros e então poderemos usá-los à vontade. Além disso, mostraremos os algoritmos para realizar operações com inteiros e algumas aplicações do estudo dos inteiros à computação. (Fica o leitor avisado que abusaremos de indicar multiplicações por justaposições dos fatores)

5.2 A relação *b divide a*

No domínio dos inteiros $\mathbb{Z}$ definimos a relação binária *b divide a* (simbologia: $b|a$) por $b|a$ *se e somente se existe* $q \in \mathbb{Z}$ *tal que* $a = bq$.

Por exemplo, $1|2$ pois $2 = 1 \cdot 2$; como 2 não é inversível, não existe inteiro q tal que $1 = 2q$ e, portanto, $\sim(2|1)$ (ou $2 \nmid 1$), exemplo que

já mostra que a relação não é simétrica. Outros exemplos: 1|(-1) e (-1)|1 e, portanto, a relação não é antissimétrica (ver proposição 2.5).

Quando *b divide a*, dizemos que *a* é *múltiplo* de *b*, que *b* é *divisor* de *a* ou que *b* é *fator* de *a*. Nesse caso, o inteiro *q* tal que $a = bq$ é chamado *quociente* de *a* por *b* e podemos escrever $q = \frac{a}{b}$, lido *a sobre b*. Observe que o quociente *q* também é um fator de *a* e que o quociente de *a* por *q* é *b*.

Proposição 1.5

A relação $b|a$ é uma relação reflexiva e transitiva.

Demonstração

A reflexividade é evidente, pois $z = z \cdot 1$ e, portanto, $z|z$ qualquer que seja o inteiro *z*. Para a transitividade, suponhamos que *m*, *n* e *p* são inteiros e $m|n$ e $n|p$. De $m|n$ e $n|p$ segue que existem inteiros q_1 e q_2 tais que $n = mq_1$ e $p = nq_2$. Daí, $p = (mq_1)q_2 = m(q_1q_2)$ e, então, $m|p$.

Proposição 2.5

Se *m* e *n* são inteiros tais que $m|n$ e $n|m$ então $m = n$ ou $m = -n$.

Demonstração

De $m|n$ e $n|m$ segue que existem q_1 e q_2 tais que $n = mq_1$ e $m = nq_2$. Daí, $n = (nq_2)q_1$ o que implica $n = n\ (q_1q_2)$. Se $n = 0$, temos

$m = 0$ e então $m = n$. Se $n \neq 0$, pela lei do corte, $1 = q_1q_2$ e, portanto, pela proposição 10.3, $q_1 = q_2 = 1$ ou $q_1 = q_2 = -1$. Logo, $m = n$ ou $m = -n$.

Proposição 3.5

Dados os inteiros a, b, c, d, a_1, ..., a_n, temos:

a) Se $b|a$ e $d|c$, então $(bd)|(ac)$.

b) Se $b|(a + c)$ e $b|a$, então $b|c$.

c) Se $b|a_1$, ..., $b|a_n$, então $b|(c_1 \cdot a_1 + ... + c_n \cdot a_n)$, quaisquer que sejam os inteiros c_1, ..., c_n.

Demonstração

a) Da hipótese, existem q_1 e q_2 tais que $a = bq_1$ e $c = dq_2$, que, multiplicadas, dão $ac = (bq_1)(dq_2) = (bd)(q_1q_2)$. Daí, $(bd)|(ac)$.

b) Da hipótese, existem q_1 e q_2 tais que $a + c = bq_1$ e $a = bq_2$. Daí, substituindo a segunda na primeira, $bq_2 + c = bq_1$, o que implica $c = b(q_1 - q_2)$. Logo, $b|c$.

c) De $b|a_i$, para $i = 1, ..., n$, segue que existem q_i, $i = 1, ..., n$, tais que $a_i = bq_i$, $i = 1, ..., n$. Daí, para quaisquer inteiros c_1, ..., c_n, $c_1a_1 + ... + c_na_n = c_1(bq_1) + ... + c_n(bq_n)$, o que resulta em $c_1a_1 + ... + c_na_n = b(c_1q_1 + ... + c_nq_n)$.

Se a_1, ..., a_n são números inteiros, uma expressão do tipo $c_1a_1 + ... + c_n \cdot a_n$, com c_1, ..., c_n inteiros, é chamada *combinação linear* de a_1, ..., a_n de *coeficientes* c_1, ..., c_n. O item (c) da proposição anterior

diz que se um inteiro b divide os inteiros a_1, ..., a_n, então b divide qualquer combinação linear desses inteiros.

5.3 Divisão euclidiana

Duas perguntas podem ser feitas: como determinar o quociente q quando $b|a$? Como saber quando $b\nmid a$? O teorema a seguir, além de responder a essas perguntas, é fundamental para o estabelecimento de uma forma inteligente de se representar os números inteiros.

Teorema 1.5 (*Divisão Euclidiana*)

Dados dois inteiros a e b, com $b \neq 0$, existem inteiros q e r tais que $a = bq + r$ e $0 \leq r < |b|$. Além disso, os inteiros q e r que satisfazem as relações acima são únicos.

Demonstração

Pela *propriedade arquimediana* discutida no corolário 5.3, existe um inteiro n tal que $n(-b) \geq -a$. Isso garante que o conjunto $S = \{z \in \mathbb{Z} | \, z \geq 0$ e $z = a - bn$, para algum $n \in \mathbb{Z}\}$ é não vazio. Como S é limitado inferiormente, pelo Princípio da Boa Ordenação, S tem um elemento mínimo r. Como $r \in S$, $r \geq 0$ e $r = a – bq$ para algum inteiro q. Ou seja, existem inteiros q e r tais que $a = bq + r$ e $r \geq 0$. Para a

primeira parte do teorema, falta mostrar que $r < |b|$. Suponhamos, por absurdo, que $r \geq |b|$. Assim, $r > r - |b| \geq 0$. Agora, de $a = bq + r$ segue $a = bq + r + |b| - |b|$, que implica $a = b(q \pm 1) + (r - |b|)$, onde "$q \pm 1$" indica a expressão "$q + 1$ ou $q - 1$". Daí, $r - |b| = a - b(q \pm 1)$, o que mostra $r - |b| \in S$, contrariando o fato de r ser o elemento mínimo de S.

Para provar que q e r são únicos, suponhamos que $a = bq_1 + r_1 = bq_2 + r_2$, com $0 \leq r_1 < |b|$ e $0 \leq r_2 < |b|$. De $r_1 < |b|$ segue que $r_1 - r_2 < |b|$, pois $- r_2 < 0$. Por outro lado, de $r_2 < |b|$ segue que $-|b| < -r_2$, o que implica $-|b| < r_1 - r_2$, pois $0 \leq r_1$. Assim $-|b| < r_1 - r_2 < |b|$ e então, pelo item (d) da proposição 9.3, $|r_1 - r_2| < |b|$.

Agora, de $bq_1 + r_1 = bq_2 + r_2$ temos que $b(q_1 - q_2) = r_2 - r_1$ e, como consequência da já citada proposição 8.3, $|b|.|q_1 - q_2| = |r_2 - r_1|$. Assim, utilizando a desigualdade $|r_1 - r_2| < |b|$ mostrada acima, $|b|.|q_1 - q_2| < |b|$ e então $|q_1 - q_2| < 1$. Daí, $|q_1 - q_2| = 0$ resultando $q_1 = q_2$. Da igualdade $b(q_1 - q_2) = r_2 - r_1$, segue $r_2 = r_1$, o que conclui a demonstração.

Na divisão euclidiana $a = bq + r$, com $0 \leq r < |b|$, a e b são, respectivamente, *dividendo* e *divisor* e q e r são o *quociente* e o *resto* da *divisão de a por b* e podem ser indicados por $q(a, b)$ e $r(a, b)$. A

divisão euclidiana de a por b pode ser indicada por $a \div b$.

Observe que se $r(a, b) = 0$, temos que $b|a$ e se $r(a, b) \neq 0$, temos $b\nmid a$ (b não divide a, para reforçar).

Por exemplo, $q(7, 3) = 2$ e $r(7, 3) = 1$, pois, é fácil ver que $7 = 3 \cdot 2 + 1$. Assim, $3\nmid 7$.

A determinação do quociente e do resto da divisão de um inteiro a por um inteiro b, no caso $a \geq 0$ e $b > 0$, pode ser feita através do seguinte algoritmo.

```
algoritmo Divisão euclidiana
   leia(a, b);
   q := 1;
   repita enquanto bq ≤ a
      q := q + 1;
   q := q - 1;
   r := a - b . q;
   escreva(q, r);
```

A propriedade arquimediana (corolário 5.3) nos garante que esse algoritmo para, pois ela assegura a existência de um inteiro z tal que $zb > a$. A interrupção do comando de repetição ocorre na primeira vez que $bq > a$, porém o comando $q := q - 1$ faz com que se retorne à desigualdade $bq \leq a$. Do comando $r := a - b \cdot q$ segue que $a = bq + r$ e o fato de que $bq \leq a$ tem como consequência $r \geq 0$. Resta mostrar que $r < b$. Se $r \geq b$, $a - bq \geq b$ e, então, $a \geq b \cdot (q + 1)$. Mas isso é uma contradição, pois q é o maior inteiro tal que $bq \leq a$.

Para exemplificar, a tabela abaixo simula a execução do algoritmo *Divisão euclidiana* para $a = 11$ e $b = 2$.

A	b	q	r
11	2	1	
		2	
		3	
		4	
		5	
		6	
		5	1

O exercício 5.2 dará indicação para determinação de quocientes e restos de divisões $a \div b$ quando $a < 0$ ou $b < 0$.

Dois resultados a respeito do quociente e do resto da divisão euclidiana de dois inteiros positivos são imediatos, mas são indispensáveis para o estabelecimento de uma forma de se representar os inteiros.

Proposição 4.5

Sejam dois inteiros a e b, com $a, b > 0$, e $q = q(a, b)$. Então

a) $q \geq 0$.

b) Se b > 1, então $a > q$.

Demonstração

a) De $a = bq + r$, com $0 \leq r < b$, segue que $a < bq + b$ o que implica $a < b(q + 1)$. Por redução ao absurdo, se $q < 0$, temos $q \leq -1$ e, então, $q + 1 \leq 0$. Daí e de $a < b(q + 1)$, $a \leq 0$, o que contraria a hipótese.

b) Do item anterior segue que $q \geq 0$. Se $q = 0$, a hipótese $a > 0$ já diz que $a > q$. Se $q > 0$, de $b > 1$ segue que $bq > q$. Daí e de $r \geq 0$, segue que $bq + r > q$ e, portanto, $a >$ q.

5.4 Sistemas de numeração

Seja b um inteiro maior que 1. Uma forma de se representar os números inteiros consiste em se adotar símbolos, chamados *algarismos*, para representar os b menores inteiros maiores do que ou iguais a zero e utilizá-los de acordo com a sua posição na representação para indicar os demais inteiros. Isto será mais bem esclarecido após o entendimento do seguinte teorema.

Teorema 2.5

Sejam os inteiros a e b, com $a > 0$ e $b > 1$. Então existem inteiros positivos n, c_0, c_1, ..., c_n, com $0 \leq c_i < b$, para todos $i = 0, 1, ..., n$, tais que $a = c_n \cdot b^n + c_{n-1} \cdot b^{n-1} + ... + c_1 \cdot b + c_0$.

Além disso, c_0, c_1, ..., c_n são únicos.

Demonstração

Pela divisão euclidiana temos que existem únicos q_0 e c_0 tais que $a = bq_0 + c_0$, $0 \leq c_0 < b$. Da mesma forma, existem únicos q_1 e c_1 tais que $q_0 = bq_1 + c_1$, $0 \leq c_1 < b$.

Seguindo esse raciocínio, obtemos $q_1 = bq_2 + c_1$, $0 \leq c_2 < b$; $q_2 = bq_3 + c_1$, $0 \leq c_3 < b$; …; $q_{n-2} = bq_{n-1} + c_{n-1}$, $0 \leq c_{n-1} < b$; $q_{n-1} = bq_n + c_n$, $0 \leq c_n < b$; …; com cada c_i e cada q_i únicos.

Pela proposição 1.5, como $a > 0$ e $b > 1$, temos que $q_i \geq 0$ e $q_{i+1} < q_i$, para todo $i = 0, 1, ..., n, ...$ Assim, obtemos uma sequência $q_0 > q_1 > ... > q_n > ... \geq 0$ e então pelo corolário 6.3, existe n tal $q_n = 0$. Logo, $q_{n-1} = c_n$ e, por substituição,

$$q_{n-2} = bc_n + c_{n-1}$$

$$q_{n-3} = b\,(bc_n + c_{n-1}) + c_{n-2} = c_n \,.\, b^2 + c_{n-1} \,.\, b + c_{n-2}$$

. . .

$$a = c_n \,.\, b^n + c_{n-1} \,.\, b^{n-1} + ... + c_1 \,.\, b + c_0$$

com c_0, c_1, ..., c_n únicos, como queríamos demonstrar.

A expressão $a = c_n \,.\, b^n + c_{n-1} \,.\, b^{n-1} + ... + c_1 \,.\, b + c_0$, com $0 \leq c_i < b$, $i = 0, 1, ..., n$, é chamada *expansão b-ádica* do inteiro a, com denominações particulares para alguns valores de b: para $b = 2$, *expansão binária*; para $b = 3$, *expansão ternária*.

Por exemplo, como

$$11 = 2 \,.\, 5 + 1,$$

$$5 = 2 \,.\, 2 + 1,$$

$$2 = 2 \,.\, 1 + 0,$$

$$1 = 2 \,.\, 0 + 1,$$

temos

$$5 = 2 \,.\, 2 + 1 = 2 \,.\, (2 \,.\, 1 + 0) + 1$$

$$5 = 1 \,.\, 2^2 + 0 \,.\, 2 + 1.$$

$$11 = 2 \,.\, 5 + 1 = 2(1 \,.\, 2^2 + 0 \,.\, 2 + 1) + 1$$

$$11 = 1 \,.\, 2^3 + 0 \,.\, 2^2 + 1 \,.\, 2 + 1,$$

e, assim, $1 \,.\, 2^3 + 0 \,.\, 2^2 + 1 \,.\, 2 + 1$ é a expansão binária de 11.

Definição: dado um inteiro $b > 1$, o *sistema de numeração de base b* é obtido definindo-se um conjunto de b símbolos (os símbolos 0 e 1 incluídos) para representar os inteiros c_i, $i = 0, 1, ..., b - 1$, com $0 \leq c_i < b$, representando-se então um inteiro positivo a de expansão b-ádica $a = c_n \,.\, b^n + c_{n-1} \,.\, b^{n-1} + ... + c_1 \,.\, b + c_0$ por $a = (c_n c_{n-1} ... c_1 c_0)_b$, onde, aí, estamos identificando c_i com o símbolo que o representa.

O inteiro $(0c_n c_{n-1} ... c_1 c_0)_b$ é identificado com o inteiro $(c_n c_{n-1} ... c_1 c_0)_b$ e um inteiro negativo é representado pelo seu simétrico precedido do sinal – (lido *menos*). Em $a = (c_n c_{n-1} ... c_1 c_0)_b$, dizemos que $c_0, ..., c_n$ são os *dígitos* ou *algarismos* de a no sistema de base b e $n + 1$ é dito *número de dígitos de a*. Dizemos também que c_0 é o

algarismo da *casa das unidades*.

É interessante observar que, como $b = 1 \,.\, b + 0$, a base b sempre é representada no sistema de base b por 10, ou seja $(b)_b = 10$.

O sistema de numeração mais utilizado é o *sistema decimal*, onde a base b é a cardinalidade do conjunto dos dedos das mãos da maioria dos seres humanos e os algarismos são 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, chamados, respectivamente, *zero*, *um*, *dois*, *três*, *quatro*, *cinco*, *seis*, *sete*, *oito* e *nove*, como já utilizamos no conjunto dos números naturais. Da mesma forma que $2 = 1 + 1$, temos $3 = 2 + 1$, $4 = 3 + 1$, $5 = 4 + 1$, $6 = 5 + 1$, e assim sucessivamente. Observe que ao se escrever $2 = 1 + 1$, estamos usando os números inteiros representados pelos algarismos 2 e 1.

A base do sistema decimal é chamada *dez* e, como foi dito acima, é representada por 10. Geralmente se omite a indicação da base quando o sistema decimal é utilizado: $(324)_{10}$ é escrito, simplesmente, 324 e é a representação do inteiro $3.10^2 + 2.10 + 4$.

Quando a representação do número inteiro no sistema decimal tem mais de três algarismos, pontos finais (ou espaços em branco) podem ser utilizados para separar, da direita para a esquerda, grupos de três algarismos. Assim, 4.324.591 é a representação do número

$$4.10^6 + 3.10^5 + 2.10^4 + 4.10^3 + 5.10^2 + 9.10^1 + 1.$$

Naturalmente, uma base *b* menor do que dez é representada pelo algarismo que representa o seu valor e os símbolos adotados são aqueles que representam os inteiros menores que a base. Assim, se a base é 7, os símbolos utilizados são 0, 1, 2, 3, 4, 5 e 6. Se a base é 2, os símbolos são 0 e 1 e o sistema é chamado *sistema binário*, fundamental para representação de inteiros em computadores. Se a base é maior que 10 é comum se utilizar letras para indicar os algarismos que representam os inteiros maiores que 9. Assim se a base é 16, os símbolos adotados são 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F.

Como

$$323 = 5.64 + 3,$$
$$64 = 5.12 + 4,$$
$$12 = 5.2 + 2,$$
$$2 = 5.0 + 2.$$

temos,

$$64 = 5.\ 12 + 4 = 5\ .\ (5\ .\ 2 + 2) + 4$$
$$64 = 2\ .\ 5^2 + 2\ .\ 5 + 4,$$
$$323 = 5\ .\ 64 + 3 = 5\ .\ (2\ .\ 5^2 + 2.\ 5 + 4) + 3$$
$$323 = 2\ .\ 5^3 + 2.\ 5^2 + 4\ .\ 5 + 3;$$

e, então, $323 = (2243)_5$. Dizemos que fizemos a *conversão* de 323 do sistema decimal para o sistema de base cinco.

Observe que o próprio enunciado do teorema 2.5 e o conceito de sistema de numeração fornecem um algoritmo para a conversão de um inteiro escrito no sistema decimal para o sistema de uma base qualquer: $z = (c_n c_{n-1} ... c_1 c_0)_b$, $c_0 = r(z, b)$, $c_1 = r(q(z, b), b)$ e, assim, sucessivamente.

Por exemplo, para se converter 45 para o sistema binário, temos

$$45 = 2 \,.\, 22 + 1,$$
$$22 = 2 \,.\, 11 + 0,$$
$$11 = 2 \,.\, 5 + 1,$$
$$5 = 2 \,.\, 2 + 1,$$
$$2 = 2 \,.\, 1 + 0,$$
$$1 = 2 \,.\, 0 + 1,$$

e, então, $45 = (101101)_2$.

A conversão de um inteiro escrito num sistema de base b qualquer para o sistema decimal é mais simples, bastando calcular, no sistema decimal, a expressão b-ádica do número. Por exemplo, como $(23501)_7 = 2 \,.\, 7^4 + 3 \,.\, 7^3 + 5 \,.\, 7^2 + 0 \,.\, 7 + 1$, temos (utilizando os algoritmos para determinação de somas e produtos de inteiros da próxima seção) que $(23501)_7 = 4.802 + 1.029 + 245 + 0 + 1$ e, então, $(23501)_7 = 6.077$.

5.5 Somas e produtos de inteiros

Tendo aprendido a representar os inteiros, vamos discutir agora algoritmos para a realização de operações com inteiros, os quais nos são ensinados (ou ensinamos) nas séries iniciais do ensino fundamental. Embora a discussão aqui colocada não deva ser passada para os alunos, é importante que um professor conheça a razão dos tais algoritmos.

Naturalmente, as operações com os números inteiros podem ser realizadas com eles representados em qualquer sistema:

(i) A soma de inteiros positivos y e z menores que a base, quando essa soma também é menor que a base, é feita utilizando a comutatividade e associatividade da soma.

Por exemplo,

$3 + 5 = 5 + 3$

$3 + 5 = 5 + (2 + 1)$

$3 + 5 = (5 + 2) + 1$

$3 + 5 = ((5 + (1 + 1)) + 1$

$3 + 5 = ((5 + 1) + 1) + 1$

$3 + 5 = (6 + 1) + 1 =$

$3 + 5 = 7 + 1 = 8$

Outro exemplo:

$(4)_7 + (2)_7 = (4)_7 + (1 + 1)_7$

$(4)_7 + (2)_7 = (4 + 1)_7 + (1)_7$

$(4)_7 + (2)_7 = (5)_7 + (1)_7 = (6)_7$.

(ii) A soma da base com um inteiro menor que ela pode ser feita utilizando-se a representação b-ádica.

Por exemplo, $10 + 4 = 1.10^1 + 4 = 14$ e $(10)_6 + (3)_6 = = 1.6^1 + 3 = (13)_6$, que corresponde a 9 no sistema decimal.

(iii) A soma de inteiros positivos *y* e *z*, menores que a base, quando essa soma é maior que a base, pode ser feita utilizando-se a igualdade $z_1 + z_2 = (z_1 + ((10)_b - z_1)) + (z_2 - ((10)_b - z_1))$, pois $z_1 + (10 - z_1) = 10$ e $z_2 - (10 - z_1) < 10$.

Por exemplo, $4 + 8 = (4 + 6) + (8 - 6) = 10 + 2 = 12$ e $(3)_7 + (6)_7 = ((3)_7 + (4)_7) + ((6)_7 - (4)_7) = (10)_7 + (2)_7 = (12)_7$.

Como $(z_1 + ((10)_b - z_1)) + (z_2 - ((10)_b - z_1)) = = (10)_b + (z_2 - ((10)_b - z_1))$, temos uma fórmula mais simples, para o caso (iii): $z_1 + z_2 = (10)_b + (z_2 - ((10)_b - z_1))$.

Por exemplo, $5 + 9 = 10 + (9 - (10 - 5)) = 10 + 4 = 14$; $6 + 4 = 10 + (4 - (10 - 6)) = 10$ e $(4)_7 + (2)_7 = (5)_8 + (6)_8 = = (10)_8 + ((6)_8 - ((10)_8 - (5)_8) = (10)_8 + ((6)_8 - (3)_8) = (10)_8 + + (3)_8 = (13)_8$, que corresponde ao decimal 11.

Evidentemente, utilizamos a nossa capacidade de memorização para decorar as somas indicadas nos casos acima. São

as *tabuadas da adição*.

Para somar operandos maiores que a base b, escrevemos suas expressões b-ádica e aplicamos as propriedades da adição. Se $x = (c_n c_{n-1}...c_1 c_0)_b$ e $y = (d_m d_{m-1}...d_1 d_o)_b$, temos, se $n > m$, $x + y = = c_n \,.\, b^n + ... + (c_m + d_m)b^m + ... + (c_1 + d_1)b + (c_0 + d_0)$.

Se $c_i + d_i < b$, não há problema. Se $c_i + d_i \geq b$, temos $(c_i + d_i)b^i = (b + (d_i - (b - c_i)))b^i = b \,.\, b^i + (d_i - (b - c_i))b^i = = b^{i+1} + (d_i - (b - c_i))b^i$ e, portanto, aparece "mais um" b^{i+1} para ser somado à soma $(c_{i+1} + d_{i+1}).b^{i+1}$. Esta é a famosa regra do "vai um".

Do exposto acima, sai o algoritmo que é ensinado nas primeiras séries do ensino fundamental para se somar $x = (c_n c_{n-1}...c_1 c_0)_b$ e $y = (d_m d_{m-1}...d_1 d_0)_b$:

1. Escreve-se os dois inteiros um abaixo do outro de modo que c_0 e d_0, c_1 e d_1 etc. fiquem numa mesma coluna.

2. Da direita para a esquerda, soma-se c_0 e d_0, c_1 e d_1 etc., escrevendo esta soma se ela for menor que a base ou escrevendo a diferença entre a soma e a base, quando aquela é maior que esta, caso em que acrescenta-se um à soma seguinte ou se escreve um se não há mais soma seguinte.

Por exemplo, para somar x = 32 767 e y = 4 581, temos

$$\begin{array}{r} 32767 \\ \underline{\ 9182} \\ 41949 \\ 168 \end{array}$$

Para somar $x = (3014)_6$ com $y = (5323)_6$, temos

$$\begin{array}{r} 3014 \\ 5323 \\ \hline 12341 \end{array}$$

Evidentemente, por associatividade, esse algoritmo pode ser generalizado para uma soma com mais de duas parcelas.

Para se calcular o produto de dois inteiros positivos y e z, menores que a base, podemos utilizar as propriedades da multiplicação e da adição. Assim,

$2 \,.\, 4 = 4 \,.\, 2 = 4 \,.\, (1 + 1) = 4 + 4 = 8;$

$3 \,.\, 8 = 8 \,.\, 3 = 8 \,.\, (2 + 1) = 8 \,.\, 2 + 8 = 8 \,.\, (1 + 1) + 8 =$
$= (8 + 8) + 8 = 16 + 8 = 24;$

$(2)_7 \,.\, (5)_7 = (5)_7 + (5)_7 = (13)_7.$

Mais uma vez, utilizamos nossa capacidade de memorização para decorar os produtos no caso acima. São as *tabuadas da multiplicação*.

Para o produto de dois inteiros quaisquer, $x = (c_n c_{n-1} \ldots c_1 c_0)_b$ e $y = (d_m d_{m-1} \ldots d_1 d_0)_b$, escrevemos suas expressões b-ádicas $x = c_n b^n + c_{n-1} b^{n-1} + \ldots + c_1 b + c_0$ e $y = d_m b^m + d_{m-1} b^{m-1} + \ldots + d_1 b + d_0$ e aplicamos a distributividade da multiplicação em relação à soma:

$xy = (c_n b^n + c_{n-1} b^{n-1} + \ldots + c_1 b + c_0)(d_m b^m + d_{m-1} b^{m-1} + \ldots + d_1 b + d_0),$

$xy = ((d_0 c_n) b^n + (d_0 c_{n-1}) b^{n-1} + \ldots + (d_0 c_1) b + (d_0 c_0)) + ((d_1 c_n) b^{n+1} + (d_1 c_{n-1}) b^n + \ldots$
$+ (d_1 c_1) b^2 + (d_1 c_0) b) + \ldots + ((d_m c_n) b^{m+n} + (d_m c_{n-1}) b^{m+n-1} + \ldots + (d_m c_1) b^{m+1} + (d_m c_0) b^m).$

Por exemplo,

$483\times34 = (4.10^2 + 8.10 + 3)(3.10^1 + 4)$

$483\times34 = ((4\times4).10^2 + (4\times8).10^1 + (4\times3)) + ((3\times4).10^3) +$
$+ (3\times8).10^2 + (3\times3).10)$,

$483\times34 = 12.10^3 + (16 + 24).10^2 + (32 + 9).10^1 + 12$,

$483\times34 = 12.10^3 + 40.10^2 + 41.10^1 + 12$,

$483\times34 = (10^4 + 2.10^3) + (4.10^3) + (4.10^2 + 1.10) + (10 + 2)$,

$483\times34 = 1.10^4 + 6.10^3 + 4.10^2 + 2.10^1 + 2$,

$483\times34 = 16.422$,

onde da quarta igualdade para a quinta usamos as igualdades

$12.10^3 = (10 + 2).10^3 = 10^4 + 2.10^3$,

$40.10^2 = (4.10).10^2 = 4.10^3$,

$41.10 = (40 + 1).10^1 = 4.10^2 + 1.10^1$.

5.6 Aplicação à Ciência da Computação: representação de caracteres em computadores

Um computador é constituído de quatro unidades básicas, denominadas *unidade de entrada*, *unidade de saída*, *unidade de processamento central* e *memória*. Uma *unidade de entrada*, como indica sua denominação, é um dispositivo pelo qual o computador

recebe os dados e as informações que ele vai manipular (o teclado, por exemplo); uma *unidade de saída* é a unidade através da qual os resultados do processamento são exibidos (o monitor ou uma impressora, por exemplo) e a *unidade de processamento central* é onde são realizadas todas as operações necessárias ao processamento. Por sua vez, a *memória* é a unidade onde os dados e as informações que serão manipulados devem ser armazenados. Naturalmente, essas quatro unidades devem se comunicar e, evidentemente, houve a necessidade de se estabelecer uma linguagem de comunicação para elas. Qualquer linguagem necessita de símbolos básicos, sendo as "palavras" da linguagem sequências desses símbolos básicos.

Na nossa linguagem escrita, usada pelos autores para comunicação com o leitor (torcemos para que sejam muitos leitores), são utilizados como símbolos básicos as *letras do alfabeto*; na linguagem falada, os símbolos básicos são os *fonemas*.

Para os computadores, considerando que os símbolos são obtidos através da ocorrência ou não de fenômenos físicos (tem corrente/não tem corrente, está magnetizado/não está magnetizado, etc.), foram adotados dois símbolos, cada um deles chamado *bit* (acrossemia de *binary digit*), representados por 0 (zero) e por 1 (um).

Assim, a comunicação entre as unidades é feita através de sequências de zeros e uns, da mesma forma que os dados são

armazenados na memória também como sequências de zeros e uns. A linguagem onde as palavras são sequências deste tipo é chamada *linguagem de máquina* e um computador só é capaz de executar instruções (e, por consequência, algoritmos) escritas em linguagem de máquina. Como essa linguagem não é corriqueira para o ser humano, cientistas da computação desenvolveram sistemas, chamados *compiladores*, capazes de traduzir instruções escritas numa linguagem comum para linguagem de máquina. Surgiram então as chamadas *linguagens de alto nível*, como *Pascal*, *C*, *Fortran*, *Java* e muitas outras. Aí, a expressão *alto nível* não está no sentido de qualidade e sim no sentido de que a linguagem está mais "próxima" do ser humano. Normalmente, um algoritmo escrito numa linguagem de alto nível é chamado *programa*.

Para que a linguagem do ser humano possa ser traduzida para a linguagem de máquina (por exemplo, este livro foi editado num processador de texto e quando estava sendo digitado, o processador de texto traduzia cada palavra para a linguagem de máquina), é necessário se estabelecer uma codificação que fixa uma sequência de *bits* para cada símbolo da nossa linguagem. Uma codificação utilizada é o *Código ASCII* (acrossemia de *American Standard Code for Information Interchange*). Nesse código, cada caractere é codificado como uma sequência de 8 bits. A sequência correspondente à letra *A*

é 01000001, a correspondente a *B* é 01000010, enquanto a sequência correspondente à letra *a* é 01100001. Naturalmente, a referência aos códigos de cada letra é facilitada vendo-se cada sequência de bits como um inteiro no sistema binário de numeração e se associando o inteiro correspondente do sistema decimal. Assim, como $(1000001)_2 = 65$, dizemos que o código ASCII decimal de *A* é 65. O código ASCII decimal de *B* é 66 e assim sucessivamente, sendo o código ASCII de *Z* igual a 90. Por outro lado, o código de *a* é $(1100001)_2 = 97$ e o da letra *z* é 122. Observe a necessidade de codificações diferentes para os padrões maiúsculo e minúsculo de uma mesma letra para que os sistemas possam encará-los como objetos distintos. Observe também que o código ASCII decimal pode ser visto como uma função do conjunto dos caracteres no conjunto dos naturais. Daqui por diante, essa função será representada por Ascii(x).

Uma questão a ser levantada: sendo Ascii(Z) = 90, por que Ascii(a) = 97 e não Ascii(a) = 91, como a "lógica sequencial" induziria? Observe que as representações das letras maiúsculas variam de 01000001 (letra A) até 01011011 (letra *Z*) e o código ASCII decimal de uma letra minúscula difere de 32 do código ASCII decimal da letra maiúscula correspondente. Isso não foi obra do acaso. Como $32 = (100000)_2$, a diferença entre as representações dos padrões

minúsculo e maiúsculo de uma mesma letra se dá apenas no segundo bit (da esquerda para direita) da representação. Levando em conta o fato de que a mudança entre os padrões maiúsculo e minúsculo é uma operação bastante utilizada nos sistemas de computação e que a mudança de um bit é uma operação muito simples de ser realizada em computadores, a escolha acima referida contribui para programas mais rápidos. Uma pergunta deixada para o leitor: por que Ascii(A) = 65 e não 1 ou 10 ou 100?

5.7 Aplicação à Ciência da Computação: representação de inteiros em computadores

Um número inteiro positivo é armazenado através da sua representação no sistema binário com uma quantidade de bits que depende do sistema de computação. Naturalmente, como o conjunto dos bits a serem utilizados é finito (suponhamos, de cardinalidade n), o subconjunto dos inteiros que podem ser armazenados tem um elemento máximo: o maior inteiro cuja representação no sistema binário tem n dígitos. A proposição a seguir fornece uma fórmula para a determinação desse maior elemento.

Proposição 5.5

O maior número inteiro do sistema decimal que possui n

dígitos no sistema binário é $z = 2^n - 1$.

Demonstração

Para que z seja o maior inteiro com *n* dígitos no sistema binário devemos ter $z = (11...1)_2$, com os *n* dígitos iguais a 1. Assim, a expansão binária de *z* é $z = 2^{n-1} + 2^{n-2} + ... + 2^1 + 1$. Como, pelo exercício 3.17,

$$a^n - b^n = (a - b)\,(a^{n-1} + a^{n-2}.b + a^{n-3}.b^2 + \ldots + a\,.\,b^{n-2} + b^{n-1}),$$

quaisquer que sejam os inteiros *a*, *b* e *n*, com $n > 1$, temos, para $a = 2$ e $b = 1$, $2^n - 1^n = (2 - 1).(2^{n-1} + 2^{n-2} + ... + 2 + 1)$ e, assim, $z = 2^n - 1$.

As formas de armazenamento de um inteiro negativo fogem ao escopo deste livro.

5.8 Aplicação à Ciência da Computação: divisão por dois em computadores

Sejam um inteiro *b*, maior que 1, e um inteiro positivo *z*, cuja representação no sistema de base *b* é $z = (c_n c_{n-1}...c_1 c_0)_b$. Assim $z = c_n b^n + c_{n-1} b^{n-1} + ... + c_1 b + c_0$ o que implica $z = (c_n b^{n-1} + c_{n-1} b^{n-2} + + ... + c_1\ )b + c_0$. Dessa forma, como $0 \leq c_0 < b$, temos que $q(z, b) = (c_n c_{n-1}...c_1)_b$ e $r(z, b) = c_0$.

Conclusão: como os números inteiros positivos são

representados em computadores pelas suas representações no sistema binário, o quociente da divisão de um inteiro positivo por dois é obtido internamente em um computador por um deslocamento de uma posição para direita dos bits e o resto da divisão de um inteiro por dois é igual ao bit da casa das unidades. Como o deslocamento para direita e a determinação do bit casa das unidades são "operações" de realizações fáceis, a divisão euclidiana por dois em computadores é uma operação bastante eficiente.

5.9 Aplicação à Ciência da Computação: um algoritmo rápido para potências

No exercício 3.16 definimos, para z, $n \in \mathbb{Z}$, $z \neq 0$ e $n \geq 0$, a *potência de base z e expoente n* por $z^n = \begin{cases} 1, \text{se } n = 0 \\ z \,.\, z^{n-1}, n > 0 \end{cases}$

No exercício referido, pedia-se para provar que

a) $a^m \,.\, a^n = a^{m+n}$.

b) $(a^m)^n = a^{m.\,n}$.

c) $a^m \,.\, b^m = (a \,.\, b)^m$.

Essas propriedades permitem que se estabeleça facilmente um algoritmo para calcular uma potência z^n, dados z e n, como vimos no capítulo 4.

Algoritmo potencia
leia(*z*, *n*);
p := 1;
i := 1;
repita enquanto n ≥ *i*
p := *p* . *z*;
i := *i* + 1;
escreva(*p*);

Por exemplo, a tabela abaixo mostra a execução desse algoritmo para $z = 3$ e $n = 5$.

z	*n*	*p*	*i*
3	5	1	1
		3	2
		9	3
		27	4
		81	5
		243	6

Quando $i = 6$, a estrutura de repetição é interrompida e o algoritmo fornece para 3^5 o valor $p = 243$.

Observe que o número de iterações da estrutura de repetição é igual ao expoente n. (Naturalmente, o número de iterações de uma estrutura de repetição de um algoritmo influi no tempo de sua execução e, por essa razão, é uma medida da *eficiência* do algoritmo).

A representação do expoente no sistema binário e as propriedades das potências podem ser utilizadas para se obter um algoritmo bem mais eficiente que o anterior.

Para se calcular x^5, podemos pensar em $x^5 = x^{1.2^2+1} =$

$= (x^2)^2 x^1$ e necessitaríamos de apenas três multiplicações: uma para calcular x^2, outra para calcular $x^4 = x^2.x^2$ e outra para calcular $x^4.x$.

De um modo geral, se queremos calcular z^n e temos $n = a_s.2^s + a_{s-1}.2^{s-1} + ... + a_1.2 + a_0$, com $a_i = 1$ ou $a_i = 0$, para todo $i = 0, 1, 2, 3, ..., s$, teremos, fatorando 2 no expoente, $z^n = (z^2)^{a_s.2^{s-1}+\cdots+ a_2.2+ a_1}.z^{a_0}$, que dá, fazendo $p_1 = z^{a_0}$, $z^n = (z^2)^{a_s.2^{s-1}+\cdots+ a_2.2+ a_1}.p_1$.

(Observe que, se $a_0 = 0$, teremos $p_1 = 1$ e p_1 não influirá no cálculo de z^n. Observe também que $a_0 = 0$ se e somente se $r(n, 2) = 0$).

Fatorando novamente 2 no expoente, obtemos $z^n = (z^4)^{a_s.2^{s-2}+\cdots+ a_2}.(z^2)^{a_1}.p_1$ e, fazendo $p_2 = (z^2)^{a_1}.p_1$, obtemos $z^n = (z^8)^{a_s.2^{s-3}+\cdots+ a_3}.(z^4)^{a_2}.p_2$.

Naturalmente, obtemos uma sequência $p_1, p_2, ..., p_s$ tal que $p_s = z^n$.

Observe que se $q_i = a_s.2^{s-i} + a_{s-1}.2^{s-(i+1)} + ... + a_i$ então, se q_{i-1} é par, $q_i = \frac{q_{i-1}}{2}$ e, se q_{i-1} é ímpar, $q_i = \frac{q_{i-1}-1}{2}$(as definições inteiros *pares* e *ímpares* encontram-se no exercício 5.7).

Para $z = 3$ e $n = 13$, por exemplo, teríamos, $3^{13} = 3^{1.2^3+1.2^2+0.2^1+1} = (3^2)^{1.2^2+1.2+0.1}.3^1$ e, então, $p_1 = 3$.

Continuando, fatorando novamente 2 no expoente,

$3^{13} = ((3^2)^2)^{1.2^1+1.1}.(3^2)^0.p_1$, e obtemos $p_2 = 1.p_1 = 3$. Repetindo o raciocínio, $3^{13} = ((3^4)^2)^{1.1}.((3^2)^2)^1.p_2$ e, então, $p_3 = ((3^2)^2)^1.p_2 = = 9^2.3 = 243$. Finalmente, $p_4 = ((3^4)^2).243$.

Temos o seguinte algoritmo.

```
algoritmo PotênciaVersao2;
   leia(z, n);
   b := z; e := n; p := 1;
   repita enquanto e ≠ 0
      se resto(e, 2) ≠ 0
         então
            p := b . p;
      e := quociente(e, 2);
      b := b . b
   escreva(p)
```

Observe que o número de multiplicações diminuiu, mas apareceram determinações de restos de divisões por dois. Porém, como foi dito na seção anterior, determinações de restos de divisões por dois são realizadas de maneira bastante rápida.

5.10 Exercícios

Para receber propostas de soluções, basta enviar e-mail para jaime@ic.ufal.br com as seguintes informações: nome completo, categoria (discente/docente), curso, instituição, estado/cidade.

5.1. Determine os quocientes e os restos das seguintes divisões.

a) $7 \div 12$

b) $(-8) \div 3$

c) $11 \div (-4)$

d) $(-10) \div (-3)$

5.2. Sejam q e r o quociente e o resto da divisão $a \div b$, $a, b > 0$. Determine os quocientes e os restos das seguintes divisões.

a) $a \div (-b)$

b) $(-a) \div (-b)$

c) $(-a) \div b$

5.3. Seja um inteiro a tal que $r(a, 5) = 4$. Determine $r(a^2, 5)$ e $q(a^2, 5)$.

5.4. Prove que se z tal que $r(z, 4) = 3$, então $r(z^2, 8) = 1$.

5.5. Sejam q e q' os quocientes e r e r' os restos das divisões $a \div b$ e $a' \div b$, $b \neq 0$. Determine o quociente e o resto da divisão $(a + a') \div b$.

5.6. Uma *ênupla* (ou *n-upla*) de elementos de um conjunto A é a imagem de uma função f do conjunto $I_n = \{1, 2, 3, \ldots, n\}$ no conjunto A. Se, para cada $i = 1, 2, \ldots, n$, representarmos por a_i a imagem $f(i)$, a ênupla será indicada por $(a_1, a_2, a_3, \ldots, a_n)$. Neste caso,

o inteiro a_i é dito *componente de ordem i*.

Se a ênupla (a_1, a_2, a_3, …, a_{348}) de inteiros contém as quantidades mensais de automóveis produzidos no Brasil no período de janeiro de 1992 a dezembro de 2020, qual o mês e o ano que correspondem à componente de ordem *k*.

5.7. Pela divisão euclidiana todo inteiro é da forma $2n$ ou da forma $2n + 1$, para algum inteiro n. Os inteiros da forma $2n$ são chamados *pares* e os da forma $2n + 1$ são chamados *ímpares*. (A qualidade de ser par ou ímpar é chamada *paridade* do inteiro). Mostre que

a) A soma (ou a diferença) de dois inteiros pares é par.

b) A soma (ou a diferença) de dois inteiros ímpares é par.

c) O produto de dois inteiros é par se um deles é par.

d) O produto de dois inteiros ímpares é ímpar.

e) Se z e n são inteiros maiores que 1, então z e z^n têm a mesma paridade.

5.8. Mostre que $z(z^{n-1} + 1)$ é par, quaisquer que sejam os inteiros z e n, com $n > 0$.

5.9. Mostre que, se x, y e z são inteiros tais que $x^2 + y^2 = z^2$, então os três inteiros são pares ou apenas um deles é par.

5.10. Mostre que todo inteiro z se escreve de modo único como $z = 3q + s$, com q inteiro e $s \in \{-1, 0, 1\}$.

5.11. Mostre que a diferença de quadrados de dois ímpares é um inteiro múltiplo de 8.

5.12. Considere os inteiros positivos m, n e a, com $m > n > 1$ e $m > a$. Determine o número de múltiplos de a menores do que ou iguais a m e o número de múltiplos de a maiores que n e menores do que ou iguais a m, ou seja, determine as cardinalidades dos conjuntos

a) $A = \{z \in \mathbb{Z} |\ 0 < z \leq m \text{ e } a|z\}$

b) $B = \{z \in \mathbb{Z} |\ n < z < m \text{ e } a|z\}$

5.13. Mostre que se a, b e n são inteiros, com $n > 0$,

a) então $(a - b)|(a^n - b^n)$.

b) e ímpar, então $(a + b)|(a^n + b^n)$.

c) e par, então $(a + b)|(a^n - b^n)$.

5.14. Mostre que se k é um inteiro positivo par, então todo inteiro da forma $z = 2^k - 1$ é múltiplo de 3.

5.15. Sejam m e n inteiros positivos, com $m > n$, e r o resto da divisão $m \div n$. Mostre que o resto da divisão $(2^m - 1) \div (2^n - 1)$ é $2^r - 1$.

5.16. Sejam n, p positivos, com $0 \leq p \leq n$. Prove que

a) $p!$ divide $n(n-1)(n-2)\ldots(n-p+1)$.

b) $(p!(n-p)!)|n!$.

Considerando o item b, definimos *número binomial n sobre p*

por $C_{n,p} = \frac{n!}{p!(n-p)!}$. (O número binomial n sobre p também pode ser representado por $\binom{n}{p}$).

5.17. Mostre que $C_{n,p} + C_{n,p+1} = C_{n+1,p+1}$, expressão conhecida como *relação de Stifel*.

5.18. Mostre que, dados a, b, $n \in \mathbb{Z}$, com $n \geq 1$, temos $(a + b)^n = a^n + C_{n,1}.a^{n-1}.b + ... + C_{n,i}.a^{n-i}.b^i + ... + b^n$, fórmula conhecida como *Binômio de Newton*.

5.19. Mostre que, para todo inteiro positivo n, $C_{n,0} + C_{n,1} + + C_{n,2} + ... + C_{n,n} = 2^n$.

5.20. Critérios de divisibilidade por 10, por 5 e por 4: seja $a = (a_n a_{n-1}...a_1 a_0)_{10}$. Mostre que

a) $10|a$ se e somente se $a_0 = 0$

b) $5|a$ se e somente se $a_0 = 0$ ou $a_0 = 5$.

c) $4|a$ se e somente se $4|(a_1 a_0)_{10}$.

5.21. Utilizando a simbologia $\underline{a}b$ para representar o número $a.10^r + b$, onde r é o número de algarismos de b, escrito no sistema decimal de numeração, mostre que $(\underline{a}5)^2 = \underline{a(a+1)}25$. (Isso significa que o quadrado de um inteiro terminado em 5 termina em 25 e os demais algarismos são os algarismos do produto do número formado pelos algarismos que precedem o 5 multiplicado pelo seu consecutivo: $35^2 = 1225$, pois $3.4 = 12$).

5.22. Mostre que se $4|k$, então o algarismo da casa das unidades de 2^k é igual a 6.

5.23. Determine em que base o número 54 do sistema decimal é representado por $(105)_b$.

5.24. Mostre que não existe base na qual o número decimal 24 é representado por $(108)_b$.

5.25. Sem realizar conversões para o sistema decimal, efetue as seguintes conversões:

a) $(11011)_2$ para o sistema de numeração de base 4.

b) $(132)_4$ para o sistema binário

5.26. Encontre um critério para verificar se um dado número representado no sistema de base b é par.

5.27. Considerando o exercício 5.10, o teorema 2.5 e o conceito de sistemas de numeração, podemos ter um sistema de numeração de base 3', com algarismos 0, 1 e $\bar{1}$, com $\bar{1}$ representando o inteiro -1. Converta o inteiro 52 do sistema decimal para o sistema de base 3'.

5.28. Mostre que com n pesos de 1 g, 3 g, 9 g, ..., 3^{n-1} g e uma balança de dois pratos pode-se avaliar qualquer massa de até $(1 + 3 + 3^2 + ... + 3^{n-1})$ g.

6. Os números primos

6.1 Introdução

Tendo construído axiomaticamente o conjunto dos números inteiros e sido apresentada uma maneira de representá-los, neste capítulo estudaremos alguns inteiros especiais, que, além de terem aplicações naturais na Matemática, são aplicados no Sistema de Criptografia RSA, objeto de estudo do capítulo seguinte. Além de estudar propriedades dos inteiros, serão vistos vários aspectos atuais e históricos da Matemática.

6.2 Máximo divisor comum

No capítulo anterior apresentamos o conceito de divisor de um número inteiro dado: b é *divisor* de a (simbologia $b|a$) se existe q tal que $a = bq$. Nesta seção, procuraremos analisar os divisores comuns de dois inteiros dados, em particular, o *maior desses divisores comuns*, chamado, por razões óbvias, de *máximo divisor comum* dos dois números e indicado por *mdc(z, y)*. Por exemplo, como os divisores positivos de 20 são 1, 2, 4, 5, 10 e 20 e os divisores de 24 são 1, 2, 3, 4, 6, 8, 12 e 24, temos mdc(20, 24) = 4.

Observe que esse exemplo já indica um algoritmo para se determinar o máximo divisor comum de dois inteiros z e y:

1. Determina-se os conjuntos $D(z)$ e $D(y)$ contendo todos os divisores de z e de y;

2. Determina-se o conjunto $D(z) \cap D(y)$;

3. Determina-se o maior elemento de $D(z) \cap D(y)$.

O problema com esse algoritmo é que, como será mostrado adiante, não existe *algoritmo eficiente* para obtenção de divisores de um número muito grande (aí, *algoritmo eficiente* significa que seja um algoritmo que forneça sua saída num tempo razoável).

Apresentaremos a seguir um algoritmo (concebido pelo matemático grego Euclides, que viveu de 330 a. C. a 275 a. C., na cidade de Alexandria, na Grécia) que calcula de forma eficiente o máximo divisor comum de dois números dados. A demonstração do *algoritmo de Euclides* requer o resultado dado no seguinte lema.

Lema 1.6

Se z, y são inteiros positivos, então $mdc(z, y) = mdc(y, z - ym)$, qualquer que seja o inteiro m.

Demonstração

Sejam $d_1 = \text{mdc}(z, y)$ e $d_2 = \text{mdc}(y, z - ym)$. Vamos mostrar que $d_2 \leq d_1$ e que $d_1 \leq d_2$ e a igualdade vem da antissimetria da relação de ordem. De $d_2 = \text{mdc}(y, z - ym)$ temos que $d_2|y$ e $d_2|(z - ym)$. Daí, $d_2|z$. Assim, d_2 é divisor comum de z e y e então

$d_2 \leq d_1$, já que $d_1 = \text{mdc}(z, y)$.

Mutatis mutandis se demonstra que $d_1 \leq d_2$ (*mutatis mutandis* é uma expressão latina que significa *mudando o que se deve*).

Observe que se tomarmos $m = q(z, y)$, temos que $z - ym = r$, onde $r = r(z, y)$. Dessa forma, temos o seguinte corolário do lema 1.6.

Corolário 1.6

Se z, y são inteiros positivos e $r = r(z, y)$, então $\text{mdc}(z, y) = \text{mdc}(y, r)$.

Com a utilização desse corolário, a determinação de mdc(20, 24) seria mdc(20, 24) = mdc(24, 20) = mdc(20, 4) = = mdc(4, 0) = 4, sendo essa última igualdade explicada pelo fato de que 4|0 e 4 é, obviamente, o maior divisor de 4.

A aplicação do corolário pode ser simplificada pelo fato de que o máximo divisor satisfaz as seguintes propriedades que decorrem imediatamente da definição e cujas demonstrações serão deixadas como exercício.

Propriedades do máximo divisor comum

a) $\text{mdc}(a, b) = \text{mdc}(|a|, |b|)$.

b) $\text{mdc}(a, b) = \text{mdc}(b, a)$.

c) Se $b|a$, então $\text{mdc}(a, b) = |b|$.

Por exemplo, mdc(504, 540) = mdc(540, 504) = = mdc(504, 36) = 36, pois 36|504.

Exemplo 2: mdc(200, 73) = mdc(73, 54) = mdc(54, 19) = =

mdc(19, 16) = mdc(16, 3) = mdc(3, 1) = 1.

Teorema 1.6 (algoritmo de Euclides)

Sejam z e y dois inteiros positivos. Se

$z = yq_1 + r_1$, com $0 \leq r_1 < y$

$y = r_1q_2 + r_2$, com $0 \leq r_2 < r_1$

$r_1 = r_2q_3 + r_3$, com $0 \leq r_3 < r_2$

$r_2 = r_3q_4 + r_4$, com $0 \leq r_4 < r_3$

. . .

$r_{n-4} = r_{n-3}q_{n-2} + r_{n-2}$, com $0 \leq r_{n-2} < r_{n-3}$

$r_{n-3} = r_{n-2}q_{n-1} + r_{n-1}$, com $0 \leq r_{n-1} < r_{n-2}$

$r_{n-2} = r_{n-1}q_n + r_n$, com $0 \leq r_n < r_{n-1}$

. . .,

então existe n tal que $r_n = 0$ e $r_{n-1} = mdc(z, y)$.

Além disso, existem t e u tais que $tz + uy = mdc(z, y)$.

Demonstração

Das desigualdades relativas aos restos, temos que $y > r_1 > r_2 > r_3 > ... > r_n > ... \geq 0$ e então, pelo corolário 5.3, existe n tal que $r_n = 0$. Por outro lado, pelo corolário 1.6, mdc(z, y) = = mdc(y, r_1) = mdc(r_1, r_2) = mdc(r_2, r_3) = … = mdc(r_{n-3}, r_{n-2}) = = mdc(r_{n-2}, r_{n-1}) = r_{n-1}.

Além disso, dessa igualdade, mdc(z, y) = r_{n-1}, segue mdc(z, y) = r_{n-3} - $r_{n-2}q_{n-1}$, na qual podemos substituir

$r_{n-2} = r_{n-4} - r_{n-3}q_{n-2}$, obtendo mdc(z, y) = $r_{n-3} - (r_{n-4} - r_{n-3}q_{n-2})q_{n-1}$. Nessa igualdade podemos substituir $r_{n-3} = r_{n-5} - r_{n-4}q_{n-3}$, e, seguindo substituindo retroativamente, encontraremos t e u tais que $tz + uy = mdc(z , y)$.

A aplicação desse algoritmo "na mão" (isto é, com lápis e papel) pode ser feita no esquema abaixo, no qual calculamos mdc(396, 84):

396	84	60	24	12	0
	4	1	2	2	

concluindo que mdc(396, 84) = 12.

Observe que esse esquema é simplesmente uma maneira prática de se realizar as divisões

$$396 = 84\times4 + 60,$$

$$84 = 60\times1 + 24,$$

$$60 = 24\times2 + 12,$$

$$24 = 12\times2 \quad \text{e} \quad r_4 = 0.$$

Para encontrar os inteiros m e n tais que $396m + 84n = 12$ temos as seguintes igualdades:

$$12 = 60 – 2\times24,$$

$$12 = 60 – 2(84 – 1\times60) = (-2)\times84 + 3\times60,$$

$$12 = (-2) \times84 + 3(396 – 84\times4) = 3\times396 – 14\times84,$$

e, portanto, $m = 3$ e $n = -14$.

É interessante observar que a recíproca da segunda parte do

teorema anterior não é verdadeira. Isto é, se *z, y* e *d* são inteiros e existem *t* e *u* tais *tz* + *uy* = *d* não se tem necessariamente *d* = *mdc*(*z*, *y*). Por exemplo, existem inteiros *t* e *u* (*t* = 2 e *u* = -2) tais que 15*t* + 10*u* = 10, mas mdc(15, 10) = 5. Mostraremos na próxima seção que essa recíproca é verdadeira quando o máximo divisor comum dos dois inteiros é igual 1.

Na linguagem algorítmica estabelecida no capítulo 4, a parte do Algoritmo de Euclides que trata da determinação do máximo divisor comum de dois inteiros (quando ambos são positivos) seria escrita da seguinte forma:

```
algoritmo deEuclides;
   leia(a, b);
   r := resto(a, b);
   repita enquanto   r > 0
      a := b;
      b := r;
      r := resto(a, b);
   mdc := b;
   escreva(mdc);
```

A eficiência desse algoritmo, que é medida pelo número de iterações do comando *repita enquanto*, será discutida no capítulo 9.

A escrita da segunda parte do Algoritmo de Euclides (a que trata da existência de inteiros *t* e *u* tais que *tz* + *uy* = *mdc*(*z*, *y*)) na linguagem algorítmica foge ao escopo do livro. (Ressaltamos que é um excelente exercício de programação de computadores).

6.3 Inteiros primos entre si

Na seção anterior, afirmamos que a recíproca da segunda parte do Algoritmo de Euclides (se $d = mdc(z, y)$, então existem inteiros t e u tais que $tz + uy = d$) só era verdadeira se $d = 1$. Ou seja, como veremos na proposição seguinte, se existem inteiros t e u tais que $tz + uy = 1$, então mdc$(z, y) = 1$. Além da veracidade dessa recíproca, o fato de o máximo divisor comum de dois inteiros ser igual a 1 é importante, pois ele gera outras propriedades interessantes. Para ampliar a linguagem matemática, quando $mdc(z, y) = 1$, dizemos que os dois inteiros z e y são *primos entre si* (ou *coprimos*) ou que um dos inteiros é *primo em relação ao outro*. Observe que dessa definição decorre que dois inteiros primos entre si não possuem divisores positivos comuns diferentes de 1 (um).

Proposição 1.6

Sejam z e y dois inteiros. Se existem inteiros t e u tais que $zt + yu = 1$, então $mdc(z, y) = 1$.

Demonstração

Seja d = mdc(z, y). Assim, $d|z$ e $d|y$ o que implica $d|(zt + yu)$. Daí, $d|1$ o que acarreta $d = 1$, já que $d > 0$.

As outras propriedades de pares de inteiros primos entre si são apresentadas na seguinte proposição.

Proposição 2.6

Sejam a, b e c inteiros positivos, com a e b primos entre si. Então

a) Se $b|(ac)$, então $b|c$.

b) Se $a|c$ e $b|c$, então $(ab)|c$.

Demonstração

a) Como a e b são primos entre si, existem inteiros m e n tais que $am + nb = 1$. Daí, multiplicando ambos os termos dessa igualdade por c, temos $amc + nbc = c$. Como b divide as duas parcelas do primeiro membro, temos $b|c$.

b) Da hipótese $a|c$, existe q_1 tal que $c = aq_1$. Assim, da hipótese $b|c$, segue que $b|(aq_1)$. Então, pelo item (a), $b|q_1$ e, portanto, existe q_2 tal que $q_1 = bq_2$. Substituindo isso em $c = aq_1$, temos que $c = abq_2$, o que mostra que $(ab)|c$.

Observe que a hipótese a e b são primos entre si é crucial para as conclusões da proposição. Por exemplo, 6|(3.8) e 6 não divide 3, nem divide 8; 3|24 e 6|24, porém 3.6 = 18 não divide 24.

6.4 Equações diofantinas

Do algoritmo de Euclides também decorre a possibilidade de se estudar um caso particular de um tipo especial de equação. Uma *equação diofantina de primeiro grau* (assim chamada em homenagem a Diophantus de Alexandria (Século IV A.C.), do qual falaremos um

pouco mais no capítulo seguinte) é uma equação do tipo $ax + by = c$, com a, b e c inteiros (chamados *coeficientes* da equação), e x e y indeterminadas no conjunto dos inteiros. Uma *solução* desta equação é um par ordenado de inteiros (k, j) tal que $ak + bj = c$.

Por exemplo, (10, -7) é uma solução da equação diofantina $5x + 7y = 1$. Por sua vez, a equação $2x + 4y = 5$ não tem solução: qualquer que seja o par de inteiros (k, j), $2k + 4j$ é par. Se uma equação diofantina tem solução, ela é dita *solúvel*.

A proposição a seguir estabelece condições para que uma equação diofantina seja solúvel.

Proposição 3.6

Sejam a e b inteiros e $d = mdc(a, b)$. A equação diofantina $ax + by = c$ é solúvel se e somente se $d|c$.

Demonstração

Suponhamos que (k, j) seja uma solução da equação $ax + by = c$. Assim, $ak + bj = c$ e daí, como $d|a$ e $d|b$, segue que $d|c$.

Reciprocamente, suponhamos que exista um inteiro t tal que $c = dt$. Do algoritmo de Euclides temos que existem inteiros m e n tais que $am + bn = d$ e, portanto, $amt + bnt = dt$. Assim, o par (mt, nt) é solução da equação $ax + by = c$.

Por exemplo, para encontrar uma solução da equação $361x + 160y = 3$, temos

361	160	41	37	4	1
	2	3	1	9	

e, então,

$1 = 37 – 9\times4,$

$1 = 37 – 9(41 - 37\times1) = -9\times41 + 10\times37,$

$1= -9\times41 + 10(160 – 41\times3) = 10\times160 – 39\times41,$

$1 = 10\times160 – 39(361 – 160\times2) = -39\times361 + 88\times160,$

$3 = (-39\times3) \times361 + (88\times3)\times160,$

$3 = -117\times361 + 264\times160.$

Portanto uma solução da equação é (-117, 264).

Encontrada uma solução de uma equação diofantina, outras soluções podem ser obtidas como mostra o seguinte corolário, cuja demonstração será deixada como exercício.

Corolário 1.6

Nas condições da proposição, se (t, u) é solução da equação $ax + by = c$, então, qualquer que seja o inteiro k, o par $\left(t - k \times \frac{b}{d}, u + k \times \frac{a}{d}\right)$ também o é (observe que $\frac{a}{d}$ e $\frac{b}{d}$ existem porque $d|a$ e $d|b$).

6.5 Números primos

Veremos agora os inteiros especiais citados na introdução deste capítulo. Veremos que há números que são os “átomos” do

conjunto dos inteiros no sentido de que são "indivisíveis" e “geram” os demais inteiros.

Seja *p* um inteiro não nulo diferente de 1 (um) e de -1 (menos um). Dizemos que *p* é *primo* se os seus únicos divisores positivos são 1 e *p*. Por exemplo, 2, 3, e -11 são primos, enquanto 35 não é primo pois 5|35. Nas condições estabelecidas acima, um número que não é primo é dito *composto*. Assim 35 é um número *composto*. Observe que 0 (zero), 1 (um) e -1 (menos um) não são primos nem são compostos. Observe a analogia entre o conceito de números primos - “não tem divisores” - e o conceito de números primos entre si - “não têm divisores comuns”. Obviamente, se *p* é primo e *p* não divide *a*, então *p* e *a* são primos entre si.

A proposição a seguir é conhecida como *propriedade fundamental dos números primos* e é utilizada por alguns autores para definir número primo. Para esses autores, a definição que nós utilizamos é estudada como uma propriedade.

Proposição 4.6

Sejam *p* um número primo e *a* e *b* inteiros positivos. Se *p*|(*ab*), então *p*|*a* ou *p*|*b*.

Demonstração

Suponhamos, por contradição, que *p* não divide *a*. Então, como *p* é primo, *a* e *p* são primos entre si. Da hipótese de que p|(ab) segue da proposição 2.6 que p|b.

No sentido de mostrar que os primos geram os inteiros, vamos mostrar que todo inteiro possui um divisor primo. Isso está discutido na seguinte proposição.

Proposição 5.6

O algoritmo abaixo, recebendo como entrada um inteiro z maior do que 1, retorna um divisor primo de z.

Algoritmo DivisorPrimo
  leia(z);
  $d := 2$;
  repita enquanto (d não divide z)
    $d := d + 1$;
  escreva(d);

Demonstração

Inicialmente, observe que o algoritmo realmente para: quando for encontrado um inteiro $d < z$, divisor de z ou quando $d = z$. Falta mostrar que d é primo. Se d não fosse primo, existiria um inteiro q tal que $1 < q < d$ e $q|d$. Como $d|z$, temos, por transitividade, que $q|z$. Porém, como o algoritmo para quando encontra o menor divisor de z, temos $d = q$, o que é uma contradição. Observe que se $d = z$, então z é primo.

Por exemplo, aplicando esse algoritmo para a entrada $z = 847$, temos a saída $d = 7$, pois $847 = 7 \times 121$, e, então, 7 é um divisor primo de 847. Aplicando o algoritmo para a entrada $z = 239$, temos a saída $d = 239$ e, portanto, 239 é primo.

Observe que o algoritmo quando a entrada é um número primo p, exige p laços. Na verdade, isso não é necessário como mostra a seguinte proposição.

Proposição 6.6

Nas condições da proposição anterior, se z não é primo, então $d^2 \leq z$

Demonstração

Como $d|z$, existe q tal que $z = dq$. Como d é o menor divisor de z, temos que $d \leq q$. Daí, de $d > 1$ segue $d.d \leq d.q$ o que resulta $d^2 \leq z$.

Essa proposição implica que se um inteiro z, maior do que 1, não possui um divisor primo p tal que $p^2 \leq z$, então ele z é primo. Assim o algoritmo poderia ser modificado para o seguinte algoritmo, que retorna um divisor primo de z, se z for composto, ou a constatação de que z é primo. Ou seja, o algoritmo abaixo, procurando o menor dos seus fatores (*fatorando-o*), verifica se um inteiro dado é ou não primo.

```
algoritmo DivisorPrimo
   leia(z);
   d := 2;
repita enquanto (d não divide z) e (d² ≤ z)
   d := d + 1;
se (d divide z)
   escreva(d 'é divisor primo de' z)
senão
```

escreva(*z* ‘é primo’);

Representando $\lfloor\sqrt{z}\rfloor$ o maior inteiro *n* tal que $n^2 \leq z$, temos que o número de laços do algoritmo acima é, no máximo, $\lfloor\sqrt{z}\rfloor$, o que ocorre quando *z* é primo. Mesmo com essa melhora o algoritmo fica muito ineficiente, se *z* é um número primo muito grande. Observe que em cada laço são efetuadas uma divisão (para verificar se *d* é divisor de *z*), uma multiplicação (para calcular d^2) e uma soma (para incrementar *d*), sem falar em comparações. Preocupando-nos apenas com a divisão (essa é a operação de realização mais demorada), suponhamos um computador que realize 10^{20} divisões por segundo. Se *z* possui 81 algarismos, então $z \geq 10^{80}$ e, portanto, $\lfloor\sqrt{z}\rfloor \geq 10^{40}$. Assim o algoritmo realizaria, no mínimo, 10^{40} laços e levaria, apenas para efetuar as divisões, $\frac{10^{40}}{10^{20}} = 10^{20}$ segundos. Esse intervalo de tempo corresponde a “aproximadamente” 10^{12} anos! Na verdade, não existe ainda um algoritmo eficiente para encontrar um fator primo de um inteiro. Vale observar que o sistema de criptografia RSA, que será estudado no capítulo seguinte, trabalha com primos com cerca de 300 algarismos.

O resultado da proposição anterior também pode ser usado para justificar o mais antigo método de geração de todos os primos positivos menores que um inteiro positivo dado, o *Crivo de Eratóstenes* (Eratóstenes foi um matemático grego que viveu,

estimadamente falando, nos anos de 284 a. C. a 250 a. C.).

Vamos descrever o Crivo de Eratóstenes para determinar todos os primos positivos menores que 300, sendo as execuções das instruções apresentadas no quadro da página seguinte.

1. Escreva o número 2 e todos os inteiros ímpares maiores do que 1 e menores que 300 (os números pares maiores que dois não são primos).

2. O número 2 é primo. Como $2^2 = 4$, todos os números menores do que 4 são primos. Daí, 3 é primo. Risque todos os múltiplos de 3: 9, 15, ..., 297.

3. Como $3^2 = 9$, todos os números menores do que 9 não riscados são primos. Daí, 2, 3, 5 e 7 também são primos. Risque todos os múltiplos de 5: 15, 25, 35, ..., 295 e todos os múltiplos de 7: 21, 35, 49, ..., 287.

4. Como $7^2 = 49$, todos os números menores do que 49 não riscados são primos. Daí, 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47 são primos. Risque todos os múltiplos desses números.

5. Como $47^2 > 300$, todos os números do crivo não riscados são primos.

(O leitor é instado a verificar nos dicionários o significado do vocábulo *crivo* e a entender a razão da sua utilização na denominação do algoritmo).

2	3	5	7	~~9~~	11	13	~~15~~	17	19
~~21~~	23	~~25~~	~~27~~	29	31	~~33~~	~~35~~	37	~~39~~
41	43	~~45~~	47	~~49~~	~~51~~	53	~~55~~	~~57~~	59
61	~~63~~	~~65~~	67	~~69~~	71	73	~~75~~	~~77~~	79
~~81~~	83	~~85~~	~~87~~	89	~~91~~	~~93~~	~~95~~	97	~~99~~
101	103	~~105~~	107	109	~~111~~	113	~~115~~	~~117~~	~~119~~
~~121~~	~~123~~	~~125~~	127	~~129~~	131	~~133~~	~~135~~	137	139
~~141~~	~~143~~	~~145~~	~~147~~	149	151	~~153~~	~~155~~	157	~~159~~
~~161~~	163	~~165~~	167	~~169~~	~~171~~	173	~~175~~	~~177~~	179
181	~~183~~	~~185~~	~~187~~	~~189~~	191	193	~~195~~	197	199
~~201~~	~~203~~	~~205~~	~~207~~	~~209~~	211	~~213~~	~~215~~	~~217~~	~~219~~
~~221~~	223	~~225~~	227	229	~~231~~	233	~~235~~	~~237~~	239
241	~~243~~	~~245~~	~~247~~	~~249~~	251	~~253~~	~~255~~	257	~~259~~
~~261~~	263	~~265~~	~~267~~	269	271	~~273~~	~~275~~	277	~~279~~
281	283	~~285~~	~~287~~	~~289~~	~~291~~	293	~~295~~	~~297~~	~~299~~

Evidentemente, a garantia de que todos os números não riscados são primos é dada pela proposição 6.6, pois cada número y não riscado não possui um divisor primo p tal que $p^2 \leq y$.

Uma simplificação pode ser efetuada nesse algoritmo, tornando-o mais eficiente (ou *menos ineficiente*). A simplificação proposta a seguir é justificada pela observação de que ao se riscar os múltiplos de um primo p, os múltiplos de p que possuem divisores menores que p já foram riscados. Dessa forma, pode-se começar a riscar os múltiplos de p a partir de p^2.

Há um algoritmo que, sem determinações de fatores, verifica se um inteiro dado é primo. Esse algoritmo é baseado no *Pequeno Teorema de Fermat*, que será discutido a seguir. Para sua

demonstração, necessitamos do seguinte lema.

Lema 1.6

Se p é um número primo e i é um inteiro tal que $1 \leq i < p$, então p é divisor de $C_{p,i}$.

Demonstração

Pela definição dada no exercício 5.15, $i!\times(p - i)!\times C_{p,i} = p!$ o que mostra que p é divisor do produto do primeiro membro. Então, pela proposição anterior, $p|i!$ ou $p|(p - 1)!$ ou $p|\ C_{p,i}$. Se ocorresse a primeira ou a segunda teríamos, pela proposição citada, $p|1$ ou $p|2$ ou ... $p|$i ou … $p|(p - 1)$, o que é um absurdo pois $k < p$, qualquer que seja $k \in \{1, 2, ..., i, ..., p - 1\}$. Logo $p|C_{p,i}$.

Teorema 2.6 (*Pequeno Teorema de Fermat*)

Se p é primo, então $p|(a^p – a)$, qualquer que seja o inteiro não nulo a.

Demonstração

Por indução, provemos inicialmente que o teorema é verdadeiro para todo inteiro $a > 0$. Para isso, seja então p um número primo e considere o predicado definido no conjunto dos inteiros positivos $P(a) = V$ se $p|(a^p – a)$.

Temos que $P(1) = V$ pois $1^p – 1 = 0$ e $p|0$ sempre. Suponhamos que $P(a) = V$ e provemos que $P(a + 1) = V$. Pela fórmula do binômio de Newton (exercício 5.17), temos que

$$(a + 1)^p - (a\ + 1)\ = (a^{p.} +\ C_{p,1}.a^{p\ -\ 1} + ... +\ C_{p,i}.a^{p\ -\ i} + ... +$$

$+ C_{p,p-1}.a + 1) - (a + 1)$,

$(a + 1)^p - (a + 1) = (a^p - a) + (C_{p,1} . a^{p-1} + ... + C_{p,,i}.a^{p-i} + ... + C_{p,p-1} . a)$, e a hipótese de indução e o lema anterior implicam $p|((a + 1)^p - (a + 1))$, como queríamos.

Agora, analisemos o caso $a < 0$. Se $p = 2$, como $a^2 - a$ é sempre par, temos $p|(a^2 - a)$; se $p \neq 2$, temos que p ímpar e, então, $|a|^p - |a| = (-a)^p - (-a) = -(a^p - a)$. Assim, como $p|(|a|^p - |a|)$, temos $p|(a^p - a)$.

Corolário 1.6

Se p é primo e a é primo em relação a p, então $p|(a^{p-1} - 1)$.

Demonstração

De $p|(a^p - a)$ segue que $p|(a . (a^{p-1} - 1))$ e, então, como p e a são primos entre si, a proposição 2.6 garante a afirmação.

Corolário 2.6

Se k é um inteiro maior que 1 e $k|(a^{k-1} - 1)$ para todo inteiro a, com $0 < a < k - 1$, então k é primo.

Demonstração

Se k é composto, então existe um primo p tal que $1 < p < k - 1$ e $p|k$. Como $p < k - 1$ temos $k|(p^{k-1} - 1)$. Daí e de $p|k$ temos $p|(p^{k-1} - 1)$, o que implica $p|1$, uma contradição.

Dessa forma o algoritmo abaixo verifica, sem fatorações, se um inteiro dado é primo.

```
algoritmo Primo
   leia(k)
   a := 2;
   repita enquanto (Resto(a^(k-1) – 1, k) = 0) e (a < k – 1))
      a := a + 1;
   se (a = k – 1)
      escreva(k 'é primo')
   senão
      escreva(k 'é composto');
```

Infelizmente (ou felizmente, dependendo do ângulo do olhar), o algoritmo acima também não é eficiente. Há bastante tempo, muitos matemáticos brilhantes vinham perseguindo a descoberta de um algoritmo que, de forma eficiente, verificasse a primalidade de um inteiro. Os esforços dispendidos foram tantos que já havia dúvidas da existência de um tal algoritmo. Em 2002, de forma surpreendente, o cientista da computação indiano Manindra Agrawal e seus alunos Neeraj Kayal e Nitin Saxena desenvolveram um algoritmo, hoje conhecido com *Algoritmo AKS*, que verifica se um número é primo de forma eficiente.

Agora mostraremos que os primos "geram" todos os números inteiros, no sentido de que todo inteiro é o produto de potências de primos.

Teorema 3.6 (Teorema Fundamental da Aritmética)

Todo inteiro $z \geq 2$ se escreve, de modo único, na forma $z = p_1^{e_1}.p_2^{e_2}.....p_k^{e_k}$, onde $p_1, p_2, ..., p_k$ são números primos tais que

$0 < p_1 < p_2 < ... < p_k$ e $e_1, e_2, ..., e_k$ são inteiros positivos.

Demonstração

Consideremos o seguinte algoritmo:

algoritmo Fatoração
  leia(z);
  $i := 1$;
  $n_i := z$;
  $q_i := 2$;
  repita enquanto $n_i > 1$
    repita enquanto (q_i não divide n_i)
      $q_i := q_i + 1$;
    escreva q_i;
    $i := i + 1$;
    $n_i := \frac{n_{i-1}}{q_{i-1}}$;
    $q_i := q_{i-1}$;

O algoritmo da proposição 5.6 garante que a estrutura de repetição interna para com q_i sendo o menor primo divisor de n_i. Assim, como q_{i+1} é divisor de $\frac{n_i}{q_i}$, $1 \leq q_i \leq q_{i+1}$ para todo i. Além disso, $n_1 > n_2 > \ldots > n_k > \ldots \geq 1$ e, então, pelo corolário 6.3, a estrutura de repetição externa para. Logo, o algoritmo acima para fornecendo os primos $q_1, q_2, \ldots, q_k$, com $q_1 \leq q_2 \leq \ldots \leq q_k$ tais que $z = q_1 . q_2 . \ldots . q_k$.

Para escrever a fatoração na forma expressa no teorema, basta fazer, quando $q_i = q_{i+1} = ... = q_{i+e_i}$, $q_i \times q_{i+1} \times ... \times q_{i+e_i} = p_i^{e_i}$, com $p_i = q_i$.

Para provar a unicidade, seja S o conjunto dos inteiros positivos que podem ser fatorados de duas maneiras distintas e suponhamos que $S \neq \emptyset$.

Como S é limitado inferiormente, pelo Princípio da Boa Ordenação, S tem um elemento mínimo n. Assim, $n = p_1^{e_1}.p_2^{e_2}.....p_k^{e_k} = q_1^{f_1}.q_2^{f_2}.....q_l^{f_l}$, onde os primos da fatoração do segundo membro são distintos dos primos da fatoração do terceiro membro ou, se os primos das duas fatorações são iguais, os expoentes correspondentes são diferentes. Ora, como $p_1|n$, temos que $p_1|(q_1^{f_1}.q_2^{f_2}.....q_l^{f_l})$ e, então, pela propriedade fundamental dos primos apresentada na proposição 4.6 (aplicada "duas vezes"), $p_1|q_j$ para algum índice j. Daí, $p_1 = q_j$ e, portanto, $n = p_1^{e_1}.p_2^{e_2}.....p_k^{e_k} = q_1^{f_1}.q_2^{f_2}.....p_1^{l_j}.....q_l^{f_l}$.

Aplicando a lei do cancelamento a essa igualdade, dividindo-a por p_1, obtemos $m = p_1^{e_1-1}.p_2^{e_2}.....p_k^{e_k} = q_1^{f_1}.q_2^{f_2}....p_1^{l_j-1}.q_l^{f_l}$ e, portanto, encontramos um inteiro m, $m < n$ (pois $m = \frac{n}{p_1}$) e que possui duas fatorações distintas, pois as duas suas fatorações acima advieram, pela simplificação por p_1, das fatorações de n que, por hipótese, são distintas. Assim, $m \in S$ o que é um absurdo, pois n é o menor elemento de S e $m < n$.

A execução do algoritmo acima para a entrada z = 5.292

geraria a seguinte tabela

i	n_i	q_i
1	5292	**2**
2	2646	**2**
3	1323	2
		3
4	441	**3**
5	147	2
		3
6	49	3
		...
		7
7	7	**7**
	1	

e a seguinte saída $q_1 = 2$, $q_2 = 2$, $q_3 = 3$, $q_4 = 3$, $q_5 = 3$, $q_6 = 7$, $q_7 = 7$. Assim $5\,292 = 2^2 \times 3^3 \times 7^2$.

A expressão $z = p_1^{e_1}.p_2^{e_2}.....p_k^{e_k}$ gerada pelo algoritmo é chamada *decomposição de z em fatores primos* e cada expoente e_k é chamado *multiplicidade* do primo p_k.

Na determinação da decomposição em fatores primos "na mão" (com lápis e papel, repetindo), a procura por divisores é feita mentalmente o que, de certa forma, simplifica as coisas. Por exemplo, a decomposição acima seria efetuada da seguinte forma:

5292	2
2646	2
1323	3
441	3
147	3
49	7
7	7
1	

Apresentamos nesta seção três algoritmos sobre números primos. O primeiro verifica se um dado número é primo, o segundo "gera" todos os primos menores que um inteiro dado e o terceiro decompõe um inteiro dado nos seus fatores primos. Outra questão a ser discutida em relação aos números primos é quanto à quantidade deles. Para isto estabeleçamos a seguinte definição. Seja p um inteiro primo positivo. O *fatorial primo* (ou *primorial*) de p é definido por $p\# = 2$, se $p = 2$ e $p\# = p \times q\#$, onde q é o maior primo menor que p, se $p > 2$. Por exemplo, $3\# = 3 \times 2\# = 3 \times 2 = 6$ e $5\# = 5 \times 3\# = 5 \times 6 = 30$. Observe que essa definição diz trivialmente que, para $p > 2$, $p\#$ é o produto de todos os primos positivos menores do que ou iguais a p.

Proposição 7.6

O conjunto dos números primos é infinito.

Demonstração

Se o conjunto dos números fosse finito haveria um primo p maior do que todos os outros primos. Naturalmente, $p > 2$. Considere

o inteiro a definido por $a = p\# - 1$. Pela proposição 5.6, a possui um divisor primo positivo q. Como estamos supondo que p é o maior primo, temos que $q \leq p$ e, portanto, q é um dos fatores de $p\#$. Assim, $q|(p\#)$ e então, como $q|a$, temos que $q|1$, o que é um absurdo. (Essa demonstração foi apresentada por Euclides, 300 a. C.!)

Sendo o número de primos infinito, uma questão seguinte a ser levantada é como os primos se distribuem ao longo do conjunto dos inteiros. Na verdade, a distribuição dos números primos é bastante irregular, podendo a diferença entre dois deles ser igual a 2, como 3 e 5, 5 e 7, 17 e 19, 239 e 241, ou ser qualquer número inteiro, pois os n inteiros $(n + 1)! + 2$, $(n + 1)! + 3$, ..., $(n + 1)! + (n + 1)$ são números compostos, para todo inteiro n: $2|((n + 1)! + 2)$, $3|((n + 1)! + 3)$, ..., $(n+1)|((n + 1)! + (n + 1))$.

Quando a diferença de dois primos é igual a 2, os primos são chamados *primos gêmeos*. Não se sabe até hoje se o número de pares de primos gêmeos é ou não finito, embora se acredite que seja infinito. Em setembro de 2016, foi encontrado um par de primos gêmeos com 388.342 dígitos (http://primes.utm.edu/top20, acessada em 28/07/2020).

6.6 Fórmulas geradoras de primos

Na História da Ciência, um sonho que sempre esteve (e sempre estará) presente na mente dos matemáticos foi (é) encontrar *fórmulas* que gerassem (gerem) números primos.

A primeira ilusão na procura de alguma fórmula geradora de primos incluía o conceito de *fatorial primo*. Como para $p > 2$, p# é sempre par temos que o único fatorial primo é 2#. É interessante observar, porém, que para todo primo p menor do que 11, (p#) + 1 é primo, conforme mostra a tabela.

p	p#	(p#) +1
2	2	3
3	6	7
5	30	31
7	210	211
11	2310	2311

Entretanto, (13#) + 1 = 30030 + 1 = 30031 = 59×509 e, então, (13#) + 1 é composto. Na verdade, são conhecidos apenas outros vinte números primos da forma (p#) + 1, sendo o maior deles (392113#)+1, com 169.966 dígitos (http://primes.utm.edu/top20, acessada em 28/07/2020).

Outras fórmulas tentadas foram as *fórmulas exponenciais* do tipo $z^n - 1$ e $z^n + 1$. Sobre o primeiro tipo temos a seguinte proposição.

Proposição 8.6

Sejam z e n inteiros maiores que 1. Se $z^n - 1$ é primo então $z = 2$ e n é primo.

Demonstração:

Do exercício 5.12 temos que $(z - 1)|(z^n - 1)$ e, daí, como $z^n - 1$ é primo, $z - 1 = 1$ ou $z - 1 = z^n - 1$. Se a segunda dessas igualdades ocorresse teríamos $z^n = z$, o que implica $z^{n-1} = 1$. Assim, teríamos $z = 1$ ou $n = 1$, valores que contrariam a hipótese "z e n inteiros maiores que 1". Logo, $z - 1 = 1$ o que implica $z = 2$.

Para provar a segunda parte da proposição, suponhamos que n não é primo. Assim, existem inteiros n_1 e n_2, com $1 < n_1 < n$ e $1 < n_2 < n$, tais que $n = n_1 n_2$. Porém, pelo exercício 5.12 e pela igualdade $(2^{n_1})^{n_2} - 1 = 2^n - 1$, temos $(2^{n_1} - 1)|(2^n - 1)$ e isto contraria o fato de que $2^n - 1$ é primo, pois $1 < 2^{n_1} - 1 < 2^n - 1$.

Os números da forma $M(n) = 2^n - 1$ são chamados *números de Mersenne.* O matemático amador Marin Mersenne (França, 1588) conjecturou que $M(n)$ seria primo para $n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$ e seria composto para os outros quarenta e quatro valores primos menores do que 257.

Um primeiro erro desta lista foi encontrado em 1886 quando se descobriu que $M(61)$ é primo. Além desse erro, também já foi provado que $M(89)$ e $M(107)$ são primos e que $M(67)$ e $M(257)$ são compostos.

Um primo da forma $M(n)$ é chamado *primo de Mersenne* e a procura por primos de Mersenne é um campo de pesquisa muito fértil em Matemática, pelo fato de que há fortes suspeitas de que os primos "gigantes" sejam dessa forma ou que, pelo menos, essa é a melhor maneira de se encontrar primos muito grandes. Há um projeto de pesquisa envolvendo pesquisadores de várias partes do mundo denominado *GIMPS* (*Great Internet Mersenne Primes Searh*- www.mersenne.org, acessada em 28/072020) cujo objetivo é encontrar primos de Mersenne.

Em 21 de dezembro de 2018, foi comprovado que o número de Mersenne $2^{82.589.933}- 1$, com 24.862.048 dígitos, é primo. Por enquanto, $2^{82.589.933}- 1$ é referido como sendo o *51° primo de Mersenne conhecido*. Nos dias que correm, o GIMPS está verificando se existe algum primo de Mersenne menor que ele ainda não descoberto. Encerrada a pesquisa, $2^{82.589.933}- 1$ será declarado o *n-ésimo primo de Mersenne*, com $n > 47$. (Já se sabe quem é o 47° primo de Mersenne: $2^{43.112.603} - 1$, com 12.837.04 dígitos. Ele foi descoberto em 12 de abril de 2009 e, na ocasião, era o 45° primo de Mersenne conhecido).

Para fórmulas exponenciais do tipo $z^n + 1$ temos a seguinte proposição.

Proposição 9.6

Sejam z e n dois inteiros maiores que 1. Se $z^n + 1$ é primo, então z é par e $n = 2^m$ para algum inteiro positivo m.

Demonstração:

Se z fosse ímpar $z^n + 1$ seria par e então não seria primo. Pela fatoração de n temos que $z = 2^m.r$, com m inteiro positivo e r ímpar e então, do exercício 5.12, $\left(z^{2^m} + 1\right) | \left(\left(2^{2^m}\right)^r + 1\right)$. Como $\left(2^{2^m}\right)^r + 1 = z^n + 1$ e este é primo, temos que $r = 1$ e $n = 2^m$, como queríamos demonstrar.

Os números da forma $F_n = 2^{2^n} + 1$ são chamados *números de Fermat*. Fermat havia conjecturado que todo número da forma F_n era primo. Observe que $F_0 = 2^1 + 1 = 3$, $F_1 = 2^2 + 1 = 5$, $F_2 = 2^4 + 1 = 17$, $F_3 = 2^8 + 1 = 257$, $F_4 = 2^{16} + 1 = 65.537$ são todos primos. Porém, no século dezoito, o matemático alemão Leonard Euler provou que $641 | F_5$ ($F_5 = 2^{32} + 1 = 4.294.967.297$) mostrando que a conjectura de Fermat era falsa.

Os únicos *primos de Fermat* conhecidos (http://mathworld.wolfram.com/FermatPrime.html, acessada em 28/07/2020) são F_0, F_1, F_2, F_3 e F_4. Todos os números de Fermat F_n com $n > 4$ estudados até agora são compostos.

6.7 A Conjectura de Goldbach

Nesta seção, falaremos brevemente sobre um dos mais antigos *problemas em aberto* (problemas para os quais não se tem uma solução, como o Algoritmo de Collatz, apresentado no capítulo 4) da Teoria dos Números. Em 7 de julho de 1742, Christian Goldbach, matemático prussiano, em uma carta que escreveu ao matemático suíço Leonard Euler fez a seguinte observação: *qualquer número ímpar maior que cinco parece ser a soma de três números primos*. Por exemplo, 7 = 2 + 2 + 3; 27 = 3 + 11 + 13; 185 = 3 + 19 + 163.

Euler verificou que a afirmação de Goldbach seria consequência da veracidade da seguinte assertiva: *todo número par maior que 2 é a soma de dois números primos*. De fato, se z é um inteiro ímpar maior que 5, então $z = x + 3$, com x par e maior que 2. Dessa forma, se x é a soma de dois primos, z é a soma de três primos.

A afirmação inicial de Goldbach, conhecida por muito tempo como *Conjectura Fraca de Goldbach* (*Conjectura Ternária de Goldbach* ou *Problema dos Três Primos)* foi demonstrada em maio de 2013 pelo matemático peruano Harald Andrés Helfgott (http://arxiv.org/pdf/1305.2897v1.pdf, acessada em 28/07/2020).

Já a asserção de Euler (conhecida hoje como *Conjectura Forte de Goldbach* ou, simplesmente, *Conjectura de Goldbach*), embora já tenha sido verificada para todos os inteiros pares menores que 4×10^{18}

(http://sweet.ua.pt/tos/goldbach.html, acessada em 07/06/2013), não foi ainda provada.

6.8 O Último Teorema de Fermat

Embora o assunto discutido aqui não tenha relação com o título do capítulo, vamos aproveitar a discussão a respeito de fatos históricos e atuais da Matemática para tecer alguns comentários sobre o Último Teorema de Fermat que, segundo Singh, *S*. (Singh 1998), foi "o enigma que confundiu as maiores mentes do mundo durante 358 anos" ou "o problema mais difícil da Terra", segundo Lynch, *J*. prefaciador da referência bibliográfica citada.

Pierre de Fermat nasceu na França em 1.601 e era matemático amador, estudando e criando matemática por puro diletantismo. Diofante de Alexandria, matemático que viveu, provavelmente, nos anos 250 *d*. *C*. escreveu treze livros sobre a teoria dos números, coleção chamada de *Aritmética*. Quando estudava o Livro II da *Aritmética* de Diofante, Fermat ficou entusiasmado com o estudo dos *trios pitagóricos*, inteiros x, y e z tais que $x^2 + y^2 = z^2$. Séculos atrás, Euclides já havia demonstrado que existe uma infinidade de trios pitagóricos (veja exercício 6.17). Em um instante de genialidade, Fermat percebeu que não existiriam inteiros x, y e z tais que $x^3 + y^3 = z^3$. Evidentemente, essa percepção foi espetacular: uma

pequena modificação de uma equação que possui uma infinidade de soluções produzia uma equação sem soluções. Fermat tentou equações com expoentes maiores e observou que elas também não tinham solução.

Na margem da *Aritmética* Fermat escreveu:

> *É impossível para um cubo ser escrito como a soma de dois cubos ou uma quarta potência ser escrita como uma soma de dois números elevado a quatro, ou, em geral, para qualquer número que seja elevado a uma potência maior do que dois ser escrito como a soma de duas potências semelhantes.*
> *Eu tenho uma demonstração realmente maravilhosa para essa proposição, mas esta margem é muito estreita para contê-la.*

Durante 350 anos, muitos matemáticos famosos tentaram demonstrar o Teorema de Fermat, o que só foi conseguido por Andrew Wiles em 1995. Esse feito ganhou manchetes na mídia internacional, tendo sido noticiado em todos os principais telejornais dos grandes países. Além disso, Wiles recebeu um prêmio de 50 mil libras de uma fundação alemã.

6.9 Exercícios

Para receber propostas de soluções, basta enviar e-mail para jaime@ic.ufal.br com as seguintes informações: nome completo, categoria (discente/docente), curso, instituição, estado/cidade.

6.1. Mostre que, qualquer que seja o inteiro n maior que 1, os pares de inteiros abaixo são primos entre si.

a) $2n + 1$ e $3n + 1$.

b) $2n + 1$ e $6n + 1$.

b) n e $n^2 + 1$.

c) $n! + 1$ e $(n + 1)! + 1$.

6.2. Mostre que 361 e 160 são primos entre si e encontre os inteiros t e u tais que $361t + 160u = 1$.

6.3. Por uma generalização lógica, o máximo divisor comum de vários números é o *maior* divisor comum destes números. Mostre que $mdc(a_1, a_2, ..., a_n) = mdc(mdc(a_1, a_2), a_3, ..., a_n)$, quaisquer que sejam os inteiros $a_1, a_2, ..., a_n$.

6.4. Sejam z e y inteiros não nulos e $d = \text{mdc}(z, y)$. Mostre que $\frac{z}{d}$ e $\frac{y}{d}$ são primos entre si.

6.5. Sejam a, b e c números inteiros. Mostre que se a e c são primos entre si, então $mdc(ab, c) = mdc(b, c)$.

6.6. Mostre que, se a e b são primos entre si, então a^m e b^n são

primos entre si, quaisquer que sejam os inteiros positivos m e n.

6.7. Mostre que se p é primo, então p *e* $(p\text{-}1)!$ são primos entre si.

6.8. Mostre que se $n > 4$ é composto, então $n|(n-1)!$.

6.9. O *mínimo múltiplo comum* de dois inteiros z e y (simbolizado por $mmc(z, y)$) é o *menor* inteiro que é múltiplo de z e de y. Sejam $m = mmc(z, y)$ e $d = mdc(z, y)$.

a) Mostre que se a é um inteiro tal que $z|a$ e $y|a$, então $m|a$.

b) Mostre que $md = zy$.

6.10. Mostre que, se a e b forem positivos, então o conjunto das soluções positivas da equação $ax + by = c$ é finito.

6.11. (Supondo conhecidos os números reais). Uma pessoa foi ao banco para descontar um cheque no valor de x reais e y centavos. O caixa do banco errou na leitura do valor do cheque e pagou y reais e x centavos. A pessoa guardou o dinheiro no bolso sem verificar a quantia. No caminho de casa, ela gastou cinco centavos e quando chegou em casa verificou que tinha exatamente o dobro do valor do cheque. Determine o valor do cheque, sabendo-se que essa pessoa não levou dinheiro nenhum consigo quando foi ao banco.

6.12. Sejam z, m e n inteiros, todos maiores que 1. Mostre que $mdc(a^m - 1, a^n - 1) = a^d - 1$, onde $d = mdc(m, n)$.

6.13. Considerando que $n! = 1\times2\times3\times \ldots \times(n\text{-}1).n$, determine a

decomposição em fatores primos de 8!.

6.14. Como foi dito na seção 6.4, um *par de primos gêmeos* é constituído de primos da forma p e $p + 2$. Naquela seção foi comentado que não se sabe se o número de pares de primos gêmeos é ou não finito. Mostre que o único *terno de primos gêmeos* é (3, 5, 7).

6.15. A primeira tentativa de se obter uma expressão que gerasse números primos foi através das funções de $\mathbb{Z}$ em $\mathbb{Z}$ da forma $f(x) = a_n x^n + ... + a_1 x + a_0$, onde a_n, ..., a_1, a_0 são números inteiros (funções deste tipo são chamadas *funções polinômios*). Essa tentativa esbarrou no fato de que se pode provar que dado um polinômio $f(x)$, existe uma infinidade de inteiros positivos m tal que $f(m)$ é composto. Prove a assertiva acima para o caso $n = 2$.

6.16. Mostre que, para todo $n > 1$,

a) $F_n = (F_{n-1} - 1)^2 + 1$.

b) $F_n = F_0 \times F_1 \times F_2 \times \ldots \times F_{n-1} + 2$.

c) Mostre que, se $m > n$, então F_m e F_n são primos entre si.

d) Use o resultado do item c para apresentar uma outra demonstração de que existem infinitos números primos.

6.17. Mostre que existe uma infinidade de *trios pitagóricos*, isto é, mostre que existe uma infinidade de conjuntos de números inteiros $\{x, y, z\}$ tais que $x^2 + y^2 = z^2$.

7. Os inteiros módulo n

7.1 Introdução

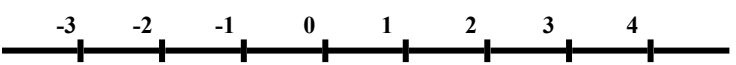
Consideremos um conjunto infinito de pontos (*ponto*, ente primitivo da Geometria Euclidiana, como visto no capítulo 1) $P = \{p_0, p_1, p_2, ..., p_n, ...\}$ de uma reta (*reta*, idem) de tal forma que:

i) os pontos da forma p_{2k+1} estão situados à direita de p_0, com $p_{2(k+1)+1}$ à direita de p_{2k+1} ($k = 0, 1, 2, ...$);

ii) os pontos da forma p_{2k} estão situados à esquerda de p_0, com $p_{2(k+1)}$ à esquerda de p_{2k} ($k = 0, 1, 2, ...$);

iii) a distância entre dois pontos consecutivos é constante (*distância*, grandeza primitiva da Física) e

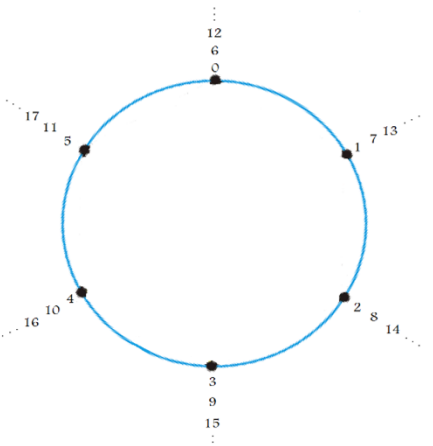
definamos a função f de P em $\mathbb{Z}$ por $f(p_i) = \frac{i+1}{2}$, se i é ímpar, e $f(p_i) = -\frac{i}{2}$, se é par. De maneira natural, a função f pode ser representada na figura, chamada *reta dos inteiros*.



Neste capítulo, vamos mostrar como, a partir do anel dos inteiros e de um inteiro $n > 1$ dado, obter um novo anel. Esses anéis serão indicados por $\mathbb{Z}_n$, são chamados *anel dos inteiros módulo n*, formalizam matematicamente os anéis I_{12} e I_7 estudados no capítulo 3

e são fundamentais para o entendimento do sistema de criptografia RSA, que estudaremos no próximo capítulo.

"Geometricamente" falando, os anéis $\mathbb{Z}_n$ são obtidos transformando a reta dos inteiros em uma circunferência, como mostra a figura, que apresenta a transformação para o caso $n = 6$.



7.2 A relação congruência módulo n

Para a construção dos anéis $\mathbb{Z}_n$, consideremos um inteiro $n > 1$ e definamos em $\mathbb{Z}$ a relação *congruência módulo n* por $a \equiv b \ mod \ n$ *se e somente se* $r(a, n) = r(b, n)$.

Por exemplo,

$25 \equiv 13 \ mod \ 4$, pois $r(25, 4) = r(13, 4) = 1$,

$35 \equiv 2 \ mod \ 3$,

$23 \equiv (-1)\ mod\ 6$,

$42 \equiv 0\ mod\ 7$.

Por seu turno, $36 \not\equiv 7\ mod\ 2$, pois $r(36, 2) = 0$ enquanto $r(7, 2) = 1$ (a simbologia $a \not\equiv b\ mod\ n$ indica que a e b não são congruentes módulo n).

Vale observar que em um contexto no qual o valor de n está fixado a expressão *mod n* pode ser omitida da simbologia.

Vale observar também que a verificação de uma congruência pela definição exige que se efetuem duas divisões. A proposição a seguir mostra que uma congruência pode ser verificada com uma subtração e uma divisão. Nesta proposição, e daqui por diante, n sempre representará um inteiro maior que 1.

Proposição 1.7

Quaisquer que sejam os inteiros a e b, $a \equiv b\ mod\ n$ se e somente se $n|(a - b)$.

Demonstração

Se $a \equiv b\ mod\ n$, então $r(a, n) = r(b, n)$ e, portanto, existem inteiros q_1 e q_2 tais que $a = nq_1 + r$ e $b = nq_2 + r$. Daí, $a - b = n(q_1 - q_2)$ e, então, $n|(a - b)$.

Reciprocamente, suponhamos que $n|(a - b)$ e sejam $r_1 = r(a, n)$ e $r_2 = r(b, n)$. Assim, $a = nq_1 + r_1$, com $0 \leq r_1 < n$ e $b = nq_2 + r_2$, com $0 \leq r_2 < n$.

Daí, $a - b = n\ (q_1 - q_2) + r_1 - r_2$ e, então, como $n|(a - b)$, $n|(r_1 - r_2)$. Logo, $n|(|r_1 - r_2|)$ o que implica $|r_1 - r_2| = 0$, pois $|r_1 - r_2| < n$. Dessa forma, $r_1 = r_2$ e $a \equiv b\ mod\ n$.

Uma consequência imediata dessa proposição relaciona a congruência módulo n com a divisão euclidiana com divisor n.

Corolário 1.7

Sejam a e r inteiros, com $0 \leq r < n$. Então $a \equiv r\ mod\ n$ se e somente se $r = r(a, n)$.

Demonstração

Suponhamos inicialmente que $a \equiv r\ mod\ n$. Daí, $n|(a - r)$ e então existe um inteiro q tal que $a - r = nq$. Assim, $a = nq + r$ e, como $0 \leq r < n$, $r = r(a, n)$.

Reciprocamente, se $r = r(a, n)$, existe um inteiro q tal que $a = nq$ + r e, então, $a - r = nq$ o que implica $n|(a - r)$ e $a \equiv r\ mod\ n$.

Como de $r = r(a, n)$ segue que $a \equiv r\ mod\ n$ é comum se dizer que $r = r(a, n)$ é o *valor de a módulo n*. Dessa forma, podemos escrever $r(a, n) =\ a\ mod\ n$ e $a\ mod\ n = b\ mod\ n$ em substituição a $a \equiv b\ mod\ n$.

Naturalmente, para $r = 0$, o corolário anterior poderia ser enunciado: $n|a$ se e somente se $a \equiv 0\ mod\ n$.

Outra consequência imediata da proposição anterior, que será usada explicitamente em uma aplicação a seguir, é dada no seguinte

corolário.

Corolário 2.7

Se a e b são inteiros e $a \equiv b \ mod \ n$, então $n|a$ se e somente se $n|b$.

Demonstração

De $a \equiv b \ mod \ n$ segue que $n|(a - b)$ e, portanto, se $n|a$ então $n|b$ e reciprocamente.

Lembramos que uma relação $\approx$ num conjunto A é dita *reflexiva* se $a \approx a$, qualquer que seja $a \in A$; é dita *simétrica* se $a \approx b$ implicar $b \approx a$, quaisquer que sejam $a, b \in A$; é dita *transitiva* se $a \approx b$ e $b \approx c$ implicar $a \approx c$, quaisquer que sejam $a, b, c \in A$. Lembramos também que uma relação que é *reflexiva*, *simétrica* e *transitiva* é chamada uma *relação de equivalência*.

Proposição 2.7

A relação de congruência é uma relação de equivalência.

Demonstração

Para mostrar a reflexividade basta ver que, como $n|0$, temos que $n|(a - a)$, qualquer que seja o inteiro a. Logo, $a \equiv a \ mod \ n$. Para a simetria basta ver que se $a \equiv b \ mod \ n$, temos $n|(a - b)$, o que implica $n|(b - a)$. Daí, $b \equiv a \ mod \ n$. Finalmente, para a transitividade, temos que se $a \equiv b \ mod \ n$ e $b \equiv c \ mod \ n$, então $n|(a - b)$ e $n|(b - c)$. Logo, $n|((a - b) + (b - c))$ o que dá $n|(a - c)$. Isso mostra que $a \equiv c \ mod \ n$.

Além de satisfazer as propriedades acima, a congruência satisfaz propriedades que podem ser relacionadas com a compatibilidade com as operações no conjunto dos inteiros, conforme mostra a seguinte proposição.

Proposição 3.7

Se $a \equiv b \ mod \ n$ e $c \equiv d \ mod \ n$, então

a) $(a + c) \equiv (b + d) \ mod \ n$.

b) $(ac) \equiv (bd) \ mod \ n$.

c) $a^m \equiv b^m \ mod \ n$, para todo inteiro positivo m.

Demonstração

a) De $a \equiv b \ mod \ n$ e $c \equiv d \ mod \ n$ segue $n|(a - b)$ e $n|(c - d)$. Daí, $n|(a - b + c - d)$ o que implica $(a + c) \equiv (b + d) \ mod \ n$, pois $a - b + c - d = (a + c) - (b + d)$.

b) De $a \equiv b \ mod \ n$ e $c \equiv d \ mod \ n$ segue $n|(a - b)$ e $n|(c - d)$. Daí, $n|(d(a - b) + a\,(c - d))$ o que implica $(ac) \equiv (bd) \ mod \ n$.

c) Provemos essa propriedade por indução sobre m.

i) A própria hipótese mostra que a afirmação é verdadeira para $m = 1$.

ii) Suponhamos que $a^k \equiv b^k \ mod \ n$ e provemos que $a^{k+1} \equiv b^{k+1} \ mod \ n$. Para isso, basta aplicar o item (b) às congruências $a \equiv b \ mod \ n$ (hipótese da proposição) e $a^k \equiv b^k \ mod \ n$ (hipótese indutiva).

O item (a) gera um corolário que será utilizado adiante.

Corolário 3.7

Se a e b são inteiros e $r_1 = a \ mod \ n$ e $r_2 = b \ mod \ n$, então $(a + b) \ mod \ n = (r_1 + r_2) \ mod \ n$.

Demonstração

De $r_1 = a \ mod \ n$ e $r_2 = b \ mod \ n$ segue $a \equiv r_1 \ mod \ n$ e $b \equiv r_2 \ mod \ n$ o que implica $(a + b) \equiv (r_1 + r_2) \ mod \ n$ e, então, $(a + b) \ mod \ n = (r_1 + r_2) \ mod \ n$.

Esse corolário permite que um resto do tipo $(a + b) \ mod \ n$ seja calculado a partir da soma dos restos $a \ mod \ n$ e $b \ mod \ n$. Basta que, no final, se calcule o valor desta soma módulo n. Por exemplo, $(22 + 19) \ mod \ 5 = (2 + 4) \ mod \ 5 = 1$.

Proposição 4.7

Sejam m e n inteiros maiores que 1 e a, b, c e d inteiros quaisquer.

a) Se $a \equiv b \ mod \ n$ e $m|n$ então $a \equiv b \ mod \ m$.

b) Se $(ac) \equiv (bc) \ mod \ n$ e $mdc(c, n) = 1$, então $a \equiv b \ mod \ n$.

c) Se $(ab) \equiv (cd) \ mod \ n$, $a \equiv c \ mod \ n$ e $mdc(a, n) = 1$, então $b \equiv d \ mod \ n$.

Demonstração

a) De $a \equiv b \ mod \ n$ segue que $n|(a - b)$. Daí, como $m|n$, temos que $m|(a - b)$ e, portanto, $a \equiv b \ mod \ m$.

b) De $(ac) \equiv (bc)\ mod\ n$, temos que $n|(c(a - b))$. Daí, como $mdc(c, n) = 1$, pela proposição 2.6, $n|(a - b)$ e a afirmação segue.

c) As duas primeiras hipóteses implicam a existência de inteiros i e j tais que $ab - cd = in$ e $a - c = jn$. Substituindo $c = a - jn$ na primeira dessas equações, obtemos $ab - ad + jnd = in$ o que implica $a\ (b - d) = (i - jd)\ n$. Daí, $n|(a(b - d))$ e então, como $mdc(a, n) = 1$, $n|(b - d)$.

Naturalmente, as assertivas dos itens (b) e (c) podem ser encaradas como *leis de cancelamento* para congruências, sendo a assertiva do item (c) uma generalização afirmação do item (b).

A relação congruência módulo n pode gerar atalhos para soluções de questões matemáticas. Por exemplo, uma forma de se provar a afirmação (ver exercício 7.0) *se* $2^k - 3^j = 7$*, então k é par* é a seguinte.

Se k fosse ímpar, de $2^k - 3^j = 7$, seguiria (considerando que $2 = 3 - 1$ e aplicando o Binômio de Newton (exercício 5.18)) $(3^k - k.3^{k-1} + ... + k.3 - 1) + 3^j = 7$, o que implicaria $3^k - k.3^{k-1} + ... + k.3 + 3^j = 8$, uma contradição, já que o primeiro membro é múltiplo de 3 e 8 não o é.

Usando congruências, bastaria observar que

$$2 \equiv (-1)\ mod\ 3 \Rightarrow 2^k \equiv (-1)^k\ mod\ 3,$$

$$3 \equiv 0\ mod\ 3 \Rightarrow 3^j \equiv 0\ mod\ 3,$$

$$7 \equiv 1\ mod\ 3,$$

e, então, de $2^k - 3^j = 7$ segue que $(-1)^k \ mod\ 3 = 1 \ mod\ 3$ e, portanto, k é par.

7.3 Uma aplicação: critérios de divisibilidade

Em um exercício do capítulo anterior, apresentamos critérios de divisibilidade por 4, por 5 e por 10. No ensino fundamental nos foi dito que para verificar se um número dado é divisível por 9 basta verificar se a soma dos seus algarismos é divisível por 9. Nesta seção provaremos esse e outros critérios de divisibilidade. Para tal, seja um inteiro z, representado no sistema decimal por $z = a_n a_{n-1}...a_1 a_0$, ou seja, seja $z = a_n \times 10^n + a_{n-1} \times 10^{n-1} + + ... + a_1 \times 10 + a_0$.

Para o critério de divisibilidade por 9, observe que $10 \equiv 1 \ mod\ 9$ e, então, pelo item (c) da proposição 3.7, $10^i \equiv 1 \ mod\ 9$, qualquer que seja o inteiro i. Daí, pelo item (b) da dessa proposição, $a_i \times 10^i \equiv a_i \ mod\ 9$, para todo $i = 0, 1, ..., n$. Assim, somando estas congruências,

$$(a_n \times 10^n + a_{n-1} \times 10^{n-1} + ... + a_1 \times 10 + a_0) \equiv (a_n + a_{n-1} + ... + a_1 + a_0) \ mod\ 9$$

e, portanto, pelo corolário 2.7,

$$9|z \text{ se e somente se } 9|(a_n + a_{n-1} + ... + a_1 + a_0).$$

Observe que o raciocínio desenvolvido continua válido para a divisibilidade por 3 já que $10 \equiv 1 \ mod\ 3$. Assim, um número é divisível

por 3 se e somente se a soma dos seus algarismos o é.

Para a divisibilidade por 11, observe que $10 \equiv (-1)$ *mod* 11 e, então, $10^i \equiv 1$ *mod* 11 se *i* é par e $10^i \equiv (-1)$ *mod* 11 se *i* é ímpar. Logo

$$(a_n \times 10^n + a_{n-1} \times 10^{n-1} + ... + a_1 \times 10 + a_0) \equiv (a_0 - a_1 + a_2 - a_3 + ...) \text{ mod } 11$$

e, portanto, um número é divisível por 11 se e somente se a *soma alternada* dos seus algarismos é divisível por 11.

7.4 Duas "mágicas" matemáticas

Da congruência

$$(a_n \times 10^n + ... + a_1 \times 10 + a_0) \equiv (a_n + ... + a_1 + a_0) \text{ mod } 9$$

e das propriedades das congruências segue que:

i) Se $z = a_n...a_1a_0$, então $(z - (a_n + ... + a_1 + a_0)) \equiv 0$ *mod* 9 donde se conclui que $9|(z - (a_n + a_{n-1} + ... + a_1 + a_0))$.

ii) Se $z = a_n...a_2a_1a_0$ e $y = b_n...b_2b_1b_0$ são tais que $b_i = a_j$, para algum *i* e algum *j*, com $0 \leq i \leq n$ *e* $0 \leq j \leq n$ (ou seja, *z* e *y* possuem exatamente os mesmos algarismos), então $9|(z - y)$.

Utilizando essas conclusões e o critério de divisibilidade por 9, é fácil, mentalmente, se descobrir o algarismo excluído no item 4 dos algoritmos a seguir.

Primeiro algoritmo:

1. Escolha um número inteiro positivo (*x*).
2. Determine a soma dos algarismos de *x* (s).

3. Determine $z = x - s$.

4. Exclua um algarismo não nulo de z.

5. Forneça, em qualquer ordem, os demais algarismos de z.

Segundo algoritmo:

1. Escolha um número inteiro positivo com algarismos distintos (x).

2. Escolha um outro inteiro com os mesmos algarismos de x (y).

3. Determine $z = |x - y|$.

4. Exclua um algarismo não nulo de z.

5. Forneça, em qualquer ordem, os demais algarismos de z.

7.5 Outra aplicação: a prova dos nove

Do raciocínio utilizado ao estabelecermos o critério de divisibilidade por 9 concluímos que se $z = a_n a_{n-1} \ldots a_1 a_0$, então $r(z, 9) = r(a_n + \ldots + a_1 + a_0, 9)$ pois

$$(a_n \times 10^n + \ldots + a_1 \times 10 + a_0) \equiv (a_n + \ldots + a_1 + a_0) \; mod \; 9.$$

O cálculo de $(a_n + a_{n-1} + \ldots + a_1 + a_0) \; mod \; 9$ pode ser facilitado pois toda vez que a soma acumulada igualar ou superar 9, podemos aplicar a congruência módulo 9, operação conhecida por *noves fora*. Por exemplo, para se calcular $r(3.289.568, 9)$, basta calcular $(3 + 2 + 8 + 9 + 5 + 6 + 8) \; mod \; 9$, o que pode ser feito da seguinte

forma:

$$3 + 2 \equiv 5,$$

$$5 + 8 \equiv 13 \equiv 4,$$

$$4 + 9 \equiv 4,$$

$$4 + 5 \equiv 0,$$

$$0 + 6 \equiv 6,$$

$$6 + 8 \equiv 5,$$

e então $r(3.289.568, 9) = 5$.

Além do dito acima, temos que se $b = b_n...b_1b_0$, então $r(ab, 9) = r((a_n + ... + a_1 + a_0)\times(b_n + ... + b_1 + b_0), 9)$,

Essas igualdades podem ser utilizadas para se demonstrar um teste de verificação de incorreção de operações com inteiros, conhecido como *prova dos nove*. Vamos mostrar o teste para a multiplicação.

Se $a = a_n...a_1a_0$, $b = b_n...b_1b_0$, $c = c_n...c_1c_0$ e $c = ab$, então se tem, $(a_n + ... + a_1 + a_0)\times(b_n + ... + b_1 + b_0) \equiv (c_n + ... + c_1 + c_0)$, módulo 9. Dessa forma, a não ocorrência dessa congruência significa que a operação não foi realizada corretamente. Para essa verificação, utilizamos o esquema

$$\begin{array}{c|c} a' & b' \\ \hline d' & c' \end{array}$$

onde

$$a' \equiv (a_n + ... + a_1 + a_0) \; mod \; 9,$$

$$b' \equiv (b_n + ... + b_1 + b_0) \; mod \; 9,$$

$$c' \equiv (c_n + ... + c_1 + c_0) \; mod \; 9 \text{ e}$$

$$d' \equiv (a'b') \; mod \; 9,$$

concluindo então que, se $c' \neq d'$, o produto não está correto. Infelizmente, a igualdade entre c' e d' não garantirá que o produto está correto, mas, evidentemente, dará uma indicação desse fato. Por exemplo, suponhamos que queiramos verificar a igualdade $425.638 \times 3.489 = 1.485.051.982$. Temos

$$a' \equiv (4 + 2 + 5 + 6 + 3 + 8) \; mod \; 9 \equiv 1,$$

$$b' \equiv (3 + 4 + 8 + 9) \; mod \; 9 \equiv 6,$$

$$c' \equiv (1 + 4 + 8 + 5 + 0 + 5 + 1 + 9 + 8 + 2) \; mod \; 9 \equiv 7,$$

$$d' \equiv (a'b') \; mod \; 9 \equiv (1 \times 6) \; mod \; 9 \equiv 6.$$

Como $c' \neq d'$, podemos garantir que a igualdade não está correta.

7.6 Potências módulo n

Nesta seção, queremos calcular potências módulo n, para algum inteiro $n > 1$. Ou seja, queremos, dados os inteiros z, m e n, com $m \geq 0$ e $n > 1$, calcular $r = (z^m, n)$ ou, ainda, queremos determinar o inteiro r, com $0 \leq r < n$, tal que $z^m \equiv r \; mod \; n$.

Em alguns casos particulares, alguns “truques” permitem

calcular potências módulo n "na mão", mesmo para n relativamente grandes. Por exemplo, para se calcular 2^{143} *mod* 17, basta observar que $2^4 \equiv (-1)$ *mod* 17 e, a partir daí, aplicar a proposição 3.7 para obter as seguintes congruências.

$$2^4 \equiv (-1) \text{ mod } 17,$$
$$(2^4)^{35} \equiv (-1)^{35} \text{ mod } 17,$$
$$2^{140} \equiv (-1) \text{ mod } 17,$$
$$2^{143} = 2^{140} \times 2^3 \equiv (-1) \times 8 \text{ mod } 17 \equiv (-8) \text{ mod } 17.$$

Finalmente, como $-8 \equiv 9$ *mod* 17, temos, pela transitividade da congruência, que $2^{143} \equiv 9$ *mod* 17 e, portanto, 2^{143} *mod* $17 = 9$.

Para se determinar 10^z *mod* 7 poderíamos usar o seguinte truque. Seja calcular 10^{45} *mod* 7. Temos, módulo 7,

$$10 \equiv 3$$
$$10^2 \equiv 30 \equiv 2$$
$$10^3 \equiv 20 \equiv 6$$
$$10^4 \equiv 60 \equiv 4$$
$$10^5 \equiv 40 \equiv 5$$
$$10^6 \equiv 50 \equiv 1,$$

e, então, $10^{45} \equiv 10^{6\times7\,+\,3} \equiv (10^6)^7 \times 10^3 \equiv 1 \times 6 \equiv 6$ e, portanto, 10^{45} *mod* $7 = 6$.

Evidentemente, os truques acima são utilizados se não se dispõe de um computador. Na prática, potências de congruências são

calculadas por um programa que implemente um algoritmo semelhante ao *algoritmo potência* apresentado no capítulo 5. Naturalmente, a única adaptação a fazer é efetuar as operações módulo *n*.

Algoritmo potência módulo n (calcula z^e *mod n*) *;*
  leia(*z*, *e*, *n*);
  b := *z*; *m* := *e*; *p* := 1;
  repita enquanto m ≠ 0
    se resto(*m*, 2) ≠ 0
      p := *b* . *p mod n*;
    m := quociente(*m*, 2);
    b := (*b* . *b*) *mod n*;
  escreva(*p*);

A tabela a seguir apresenta a execução desse algoritmo para o cálculo de 3^{99} *mod* 29.

a	*e*	*n*	*b*	*m*	*p*
3	99	29	3	99	1
			r(3 . 3, 29) = 9	q(99, 2) = 49	r(1 . 3, 29) = 3
			r(9 . 9, 29) = 23	q(49, 2) = 24	r(9 . 3, 29) = 27
			r(23 . 23 , 29) = 7	q(24, 2) = 12	
			r(7 . 7, 29) = 20	q(12, 2) = 6	
			r(20 . 20, 29) = 23	q(6, 2) = 3	
			r(23 . 23, 29) = 7	q(3, 2) = 1	r(23 . 27, 29) = 12
			r(7 . 7, 29) = 20	q(1, 2) = 0	r(7 . 12, 29) = 26

e, assim, 3^{99} *mod* 29 = 26.

7.7 Os inteiros módulo n

De um modo geral, se A é um conjunto, $\approx$ é uma relação de equivalência em A e a é um elemento de A, *a classe de equivalência de a pela relação* $\approx$ é o conjunto $\bar{a} = \{x \in A | x \approx a\}$. Por exemplo, para a relação definida no exercício 2.4 (definida em $\mathbb{N}\times\mathbb{N}$ por $(m, n) \approx (p, q)$ *se e somente se* $m + q = n + p$) temos:

$\overline{(1,1)} = \{(n, m) \in \mathbb{N}\times\mathbb{N} | m = n\}$.

$\overline{(1,2)} = \{(n, m) \in \mathbb{N}\times\mathbb{N} | m = n + 1\}$.

Proposição 5.7

Sejam A um conjunto e $\overline{a}$ e $\overline{b}$ classes de equivalência em relação a uma relação de equivalência $\approx$. Então

a) $a \in \overline{a}$.

b) $\overline{a} = \overline{b}$ se e somente se $a \approx b$.

c) Se $\overline{a} \neq \overline{b}$, então $\overline{a} \cap \overline{b} = \emptyset$.

Demonstração

a) Decorre imediatamente da reflexividade de $\approx$.

b) Suponhamos que $\overline{a} = \overline{b}$. Como, pelo item (a), $a \in \bar{a}$ temos que $a \in \bar{b}$. Daí, $a \approx b$. Reciprocamente, suponhamos $a \approx b$ e tomemos $x \in \bar{a}$. Daí, $x \approx a$ e, por transitividade, $x \approx b$, o que implica $x \in \bar{b}$. Assim $\bar{a} \subset \bar{b}$. *Mutatis mutandis*, se mostra

que $\bar{b} \subset \bar{a}$.

c) Se $\bar{a} \cap \bar{b} \neq \emptyset$, existe $x \in \bar{a}$ e $x \in \bar{b}$ o que implica que a existência de $x \in A$ tal que $x \approx a$ e $x \approx b$. Daí, por reflexividade e transitividade, $a \approx b$ e, então, pelo item (b), $\bar{a} = \bar{b}$. Porém, isso contraria a hipótese.

As classes de equivalência da relação *congruência módulo n* são chamadas *classes residuais módulo n* e qualquer inteiro *b* tal que $\bar{a} = \bar{b}$ é dito *um representante* da classe residual $\bar{a}$.

Por exemplo, existem duas classes residuais módulo 2:

$\bar{0}$ = {..., -4, -2, 0, 2, 4, ...}

$\bar{1}$ = {..., -3, -1, 1, 3, ...}

e, portanto, qualquer número par é representante da classe $\bar{0}$ e qualquer número ímpar é representante da classe $\bar{1}$.

De forma semelhante, existem três classes residuais módulo 3. A classe $\bar{0}$ que contém os múltiplos de 3, a classe $\bar{1}$ que tem como representantes os inteiros da forma $3q + 1$ e a classe $\bar{2}$ com representantes da forma $3q + 2$.

O fato de existirem duas classes residuais módulo 2 e três classes residuais módulo 3 não é privilégio desses dois inteiros, como mostra a seguinte proposição.

Proposição 6.7

Existem exatamente n classes residuais módulo n: $\overline{0}, \overline{1}, ..., \overline{(n-1)}$.

Demonstração

Provemos inicialmente as n classes listadas são diferentes. Ou seja, provemos que se $0 \leq a < n$, $0 \leq b < n$ e $a \neq b$, então $\overline{a} \neq \overline{b}$. De fato, se $\overline{a} = \overline{b}$, então, pela proposição anterior, $a \equiv b \ mod \ n$ e daí, como $0 \leq b < n$, $b = r(a, n)$. Da mesma forma, como $0 \leq a < n$, temos que $a = r(a, n)$ e, portanto, pela unicidade do resto, $a = b$, o que é uma contradição.

Agora, dado qualquer inteiro a, pela divisão euclidiana, existem inteiros q e r tais que $a = nq + r$, com $0 \leq r < n$. Assim, $a \equiv r \ mod \ n$, o que implica $\overline{a} = \overline{r}$. Portanto, como $0 \leq r < n$, $\overline{a}$ é uma das classes $\overline{0}, \overline{1}, ..., \overline{(n-1)}$.

O conjunto das classes residuais módulo n $\{\overline{0}, \overline{1}, ..., \overline{(n-1)}\}$ é indicado por $\mathbb{Z}_{\mathbf{n}}$ e é denominado *conjunto dos inteiros módulo n*. É habitual, em um contexto em que n está fixado, omitirmos as barras nas indicações das classes residuais, identificando, então, os conjuntos $\mathbb{Z}_n$ e I_n, já que $\overline{n} = \overline{0}$.

Em $\mathbb{Z}_n$ definimos as seguintes operações, utilizando, nos segundos membros, os mesmos operadores + e . das operações em $\mathbb{Z}$.

i) Adição: $\bar{a} + \bar{b} = \overline{a+b}$

ii) Multiplicação: $\bar{a}.\bar{b} = \overline{a.b}$

Evidentemente, é necessário garantir que essas operações estão *bem definidas* no sentido de que uma soma ou um produto de classes residuais independem do particular representante da classe que foi utilizado. Isso significa que devemos provar que se $x \in \bar{a}$ e $y \in \bar{b}$, então $\overline{x+y} = \overline{a+b}$ e $\overline{x.y} = \overline{a.b}$. Essas igualdades, porém, decorrem da proposição 3.7, pois $x \in \bar{a}$ e $y \in \bar{b}$ implicam $x \equiv a \ mod \ n$ e $y \equiv b \ mod \ n$ e, então, a referida proposição garante que $(x + y) \equiv (a + b) \ mod \ n$ e $(x.y) \equiv (a.b) \ mod \ n$.

Teorema 1.7

$\mathbb{Z}_n$ munido das operações definidas acima é um anel.

Demonstração

A associatividade e a comutatividade da adição e da multiplicação decorrem de imediato da associatividade e da comutatividade da adição e da multiplicação dos inteiros. De fato, por exemplo, $\bar{a} + \bar{b} = \overline{a+b} = \overline{b+a} = \bar{b} + \bar{a}$ e $\bar{a}.(\bar{b}.\bar{c}) = \bar{a}.\overline{b.c} =$ $= \overline{a.(b.c)} = \overline{(a.b).c} = \overline{a.b}.\bar{c} = (\bar{a}.\bar{b}).\bar{c}$.

O elemento neutro da adição é $\bar{0}$, pois $\bar{a} + \bar{0} = \overline{a+0} = \bar{a}$ e o elemento neutro da multiplicação é $\bar{1}$, pois $\bar{a}.\bar{1} = \overline{a.1} = \bar{a}$. O simétrico de uma classe $\bar{a}$ é classe $\overline{n-a}$, pois $\bar{a} + \overline{n-a} =$ $= \overline{a+(n-a)} = \bar{n} = \bar{0}$. A distributividade da multiplicação em

relação à adição também é simples de provar e decorre da propriedade respectiva do anel dos inteiros.

As tabelas das operações em $\mathbb{Z}_2 = \{0, 1\}$ são

+	0	1
0	0	1
1	1	0

.	0	1
0	0	0
1	0	1

enquanto as tabelas das operações em $\mathbb{Z}_3 = \{0, 1, 2\}$ são

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

.	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Por seu turno, as tabelas para $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ são

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

.	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Observe que $\mathbb{Z}_4$ não é um domínio de integridade, pois $\bar{2}.\bar{2} = \bar{0}$, enquanto que $\mathbb{Z}_3$ o é. Observe também que em $\mathbb{Z}_4$ o inverso de $\bar{3}$ é o próprio $\bar{3}$ e que $\bar{2}$ não tem inverso: não existe a tal que $\bar{2}.\bar{a} = \bar{1}$.

É simples realizar operações em $\mathbb{Z}_n$ mesmo que n seja grande. Basta observar que $\bar{a}.\bar{b} = \bar{r}$, onde $r = r(ab, n)$. Foi assim que foram

feitas as tabelas da multiplicação e da adição do $\mathbb{Z}_{12}$ apresentadas no capítulo 3, representado na ocasião por I_{12} e sendo utilizado 12 para representar $\bar{0}$. Se você observar as tabelas referidas vai observar que em $\mathbb{Z}_{12}$ 2, 3, 4, 6, 8, 9 e 10 não têm inversos e que $5^{-1} = 5$ e $7^{-1} = 7$, $11^{-1} = 11$. É fácil ver que em $\mathbb{Z}_3$ e em $\mathbb{Z}_5$ todo elemento não nulo tem inverso e que $2^{-1} = 2$ em $\mathbb{Z}_3$ e $3^{-1} = 2$ em $\mathbb{Z}_5$.

A proposição a seguir estabelece as condições para que um elemento de $\mathbb{Z}_n$ seja inversível e sua demonstração fornece um algoritmo para a determinação do inverso de um elemento inversível.

Proposição 7.7

Um elemento $a \in \mathbb{Z}_n$ é inversível se e somente se a e n são primos entre si.

Demonstração

Suponhamos que $a \in \mathbb{Z}_n$ é inversível. Então existe $b \in \mathbb{Z}_n$ tal que $ab \equiv 1 \ mod \ n$. Assim, $n|(ab - 1)$ e, daí, existe $t \in \mathbb{Z}$ tal que $ab - 1 = nt$. Concluímos então que existem inteiros b e t tais que $ab + nt = 1$, o que implica, pela proposição 1.6, que a e n são primos entre si.

Reciprocamente, se $mdc(a, n) = 1$, existem inteiros b e t tais que $ab + nt = 1$. Daí, $ab = nt + 1$, o que implica $ab \equiv 1 \ mod \ n$. Logo, em $\mathbb{Z}_n$, $ab = 1$ e a é inversível.

Como foi dito acima, essa demonstração embute um algoritmo

para se determinar o inverso de um elemento inversível a de $\mathbb{Z}_n$: basta se determinar os inteiros b e t tais que $ab + nt = 1$, o que pode ser feito pelo algoritmo de Euclides. Por exemplo, para se determinar o inverso de 63 em $\mathbb{Z}_{176}$ calculamos $mdc(176, 63)$

176	63	50	13	11	2	1
	2	1	3	1	5	

e, portanto, 63 é inversível. Para determinar o seu inverso temos

$$1 = 11 - 5\times2$$

$$1 = 11 - 5(13 - 1\times11) = -5\times13 + 6\times11$$

$$1 = -5\times13 + 6(50 - 3\times13) = 6\times50 - 23\times13$$

$$1 = 6\times50 - 23(63 - 1\times50) = -23\times63 + 29\times50$$

$$1 = -23\times63 + 29(176 - 2\times63) = 29\times176 - 81\times63.$$

Daí, $b = -81$ e $63^{-1} = -81 = 176 - 81 = 95$. Observe que, de fato, $63\times95 = 5985 \equiv 1 \ mod \ 176$.

A determinação do inverso de 13 em $\mathbb{Z}_{40}$ seria bem mais simples: como

40	13	1
	3	

temos $1 = 40 - 13\times3$ e, então, $13^{-1} = -3 = 40 - 3 = 37$.

Corolário 4.7

Se p é um inteiro primo positivo, então todo elemento não nulo de $\mathbb{Z}_p$ é inversível.

Demonstração

Como p é primo, temos que $mdc(p, i) = 1$, para todo $i = 1, 2,$

3, ..., $p - 1$. Logo $\overline{1}, \overline{2}, ..., \overline{p-1}$ são inversíveis.

Corolário 5.7

Sejam $k = p^n$, com p *e* n inteiros positivos, p primo, e m um inteiro positivo tal que $m \leq k$. Então $\overline{m}$ não é inversível em $\mathbb{Z}_k$ se e somente se $m = ip$ para algum $i = 1, 2, 3, \ldots, p^{n-1}$.

Demonstração

Seja $d = mdc(m, k)$. Se $m = ip$ para algum $i = 1, 2, 3, \ldots, p^{n-1}$, então $d \geq p > 1$ e $\overline{m}$ não é inversível em $\mathbb{Z}_k$. Reciprocamente, se $\overline{m}$ não é inversível em $\mathbb{Z}_k$, então $d > 1$. Como p é primo, $d = p^j$ para algum $1 \leq j < p$. Assim, $(p^j)|m$ para algum $1 \leq j < p$, o que implica $m = tp^j$, para algum$1 < j < p$ e algum inteiro t. Dessa forma, $m = (tp^{j-1})p$ para algum $1 \leq j < p$ e algum inteiro t, o que implica o que queremos, pois $m \leq p^n$.

7.8 Congruências Lineares

Sejam a, b e n números inteiros, com $n > 1$, e x uma indeterminada em $\mathbb{Z}$. Uma *congruência linear módulo n* é uma congruência do tipo $ax \equiv b \ mod \ n$. Um inteiro x_0 tal que $ax_0 \equiv b \ mod \ n$ é dito uma *solução* da congruência. Por exemplo, $x_0 = 15$ é uma solução da congruência $3x \equiv 5 \ mod \ 8$, pois $45 \equiv 5 \ mod \ 8$.

Por transitividade, se x_0 é uma solução da congruência $ax \equiv b \ mod \ n$ e $x_1 \equiv x_0 \ mod \ n$ então x_1 também é solução. Portanto, as soluções de uma congruência linear se dividem em classes residuais módulo n.

Observe que a congruência $ax \equiv b \ mod \ n$ é equivalente à equação $\bar{a}.\bar{x} = \bar{b}$. Assim, uma classe residual solução da equação $\bar{a}.\bar{x} = \bar{b}$ é dita também uma *solução módulo n* da congruência $ax \equiv b \ mod \ n$.

É muito fácil ver que se a e n são primos entre si, então a congruência $ax \equiv b \ mod \ n$ tem uma única solução módulo n. De fato, da hipótese de que a e n são primos entre si segue que $\bar{a}$ é inversível em $\mathbb{Z}_n$ e, assim, $x_0 = (\overline{a})^{-1}\bar{b}$ é a solução única da congruência.

Por exemplo, como $\left(\overline{3}\right)^{-1} = \bar{3}$, temos que $x_0 = \left(\overline{3}\right)^{-1} \times \bar{5} = \bar{3} \times \bar{5} = \bar{7}$ é a única solução da congruência $3x \equiv 5 \ mod \ 8$.

Uma congruência do tipo $(ax + c) \equiv b \ mod \ n$ também é uma congruência linear, pois ela equivalente à congruência $ax \equiv (b - c) \ mod \ n$. Por exemplo, $(5x + 9) \equiv 7 \ mod \ 6$ é equivalente à $5x \equiv (-2) \ mod \ 6 \equiv 4 \ mod \ 6$. Como em $\mathbb{Z}_6$, $\left(\overline{5}\right)^{-1} = \bar{5}$, temos que $x \equiv (5 \times 4) \ mod \ 6 \equiv 2 \ mod \ 6$, e, portanto, $\bar{2}$ é a única solução da congruência do exemplo.

Quando a e n não são primos entre si, temos a seguinte proposição.

Proposição 8.7

Sejam a, b e n números inteiros, com $n > 1$ e $d = mdc(a, n)$. A congruência linear $ax \equiv b \ mod \ n$ tem solução se e somente se $d|b$.

Demonstração

Suponhamos que exista um inteiro x_0 tal que $ax_0 \equiv b \ mod \ n$. Então $n|(ax_0 - b)$ e, portanto, existe um inteiro y_0 tal que $ax_0 - b = ny_0$. Daí, como $d|a$ e $d|n$, segue que $d|b$.

Reciprocamente, suponhamos que $d|b$. Assim, existe q tal que $b = dq$. Por outro lado, como $d = mdc(a, n)$, existem inteiros x_0 e y_0 tais que $ax_0 + ny_0 = d$. Daí, $ax_0q + ny_0q = dq = b$ e, portanto, x_0q é uma solução da congruência $ax \equiv b \ mod \ n$.

Por exemplo, consideremos a congruência $6x \equiv 4 \ mod \ 8$. Como $mdc(6, 8) = 2$, $\overline{6}$ não é inversível em $\mathbb{Z}_8$. Porém, como $2|4$, a congruência tem solução. Temos, aplicando o algoritmo de Euclides para o cálculo de $mdc(6, 8) = 2$,

8	6	2
	1	3

e, então, $2 = 8 - 6 \times 1$. Portanto, $4 = 2 \times 8 + 6 \ (-2)$ o que mostra que $6(-2) \equiv 4 \ mod \ 8$. Daí, $x_0 = \overline{-2} = \overline{6}$ é uma solução da congruência. Da igualdade $2 = 8 - 6 \times 1$, segue também $2 + (-6) = 8 - 6 \times 1 + (-6)$, que dá $-4 = 8 - 6 \times 2$. Esta igualdade mostra que $6 \times 2 \equiv 4 \ mod \ 8$ e, então, $\overline{2}$ é

outra solução da congruência.

Observe que essa demonstração foi baseada no fato óbvio de que a congruência $ax \equiv b \ mod \ n$ tem solução se e somente se a equação diofantina $ax + nq = b$ tem solução, o que foi visto na proposição 3.6.

Imagine agora que queiramos determinar um número inteiro que ao ser dividido por 11 e por 13 deixe restos respectivamente iguais a 1 e 2. Evidentemente, a solução desse problema está em se determinar um inteiro x que satisfaça as congruências:

$$x \equiv 1 \ mod \ 11,$$

$$x \equiv 2 \ mod \ 13.$$

Um conjunto de congruências lineares como esse é chamado de um *sistema de congruências lineares*. Para encontrar uma solução do sistema acima, basta observar que da primeira congruência segue que existe um inteiro t tal que $x = 11t + 1$. Substituindo x na segunda congruência, encontramos $(11t + 1) \equiv 2 \ mod \ 13$, donde segue, $11t \equiv 1 \ mod \ 13$.

Como em $\mathbb{Z}_{13}$, $\left(\overline{11}\right)^{-1} = \bar{6}$, temos $t \equiv 6 \ mod \ 13$ e, então, $t = 13u + 6$, para u inteiro. Substituindo t em $x = 11t + 1$, temos $x = 143u + 67$ e, portanto, um dos números procurados é 67.

Imagine agora que queiramos um inteiro x que deixe restos iguais a 1 e a 2 quando dividido por 9 e por 12, respectivamente. Temos, como acima, que

$x \equiv 1 \ mod \ 9,$

$x \equiv 2 \ mod \ 12.$

Da primeira segue $x = 9t + 1$, para algum inteiro t, e da segunda, por substituição de x, $9t + 1 \equiv 2 \ mod \ 12$. Daí, $9t \equiv 1 \ mod \ 12$. Porém, como $mdc(9, 12) = 3$ e 3 não divide 1, temos que a congruência acima não tem solução e, portanto, não existe o inteiro procurado.

O teorema a seguir (conhecido como *Teorema do Resto Chinês*) discute as condições de existência de soluções de sistemas de congruências lineares.

Teorema 2.7 (Teorema do Resto Chinês)

Sejam $n_1, n_2, ..., n_k$ inteiros positivos dois a dois primos entre si. Se $a_1, a_2, ..., a_k$ são inteiros, então o sistema de congruências lineares

$x \equiv a_1 \ mod \ n_1$

$x \equiv a_2 \ mod \ n_2$

...

$x \equiv a_k \ mod \ n_k$

tem uma única solução módulo $n_1 \times n_2 \times ... \times n_k$.

Demonstração

Demonstraremos o teorema para $k = 2$. O caso geral se demonstra de forma muito semelhante e será deixada como exercício.

Sejam m e n inteiros tais que $mdc(m, n) = 1$ e a e b dois inteiros quaisquer. Queremos provar que o sistema

$$x \equiv a \ mod \ n$$

$$x \equiv b \ mod \ m$$

tem uma única solução módulo mn.

Da primeira equação temos que $x = nt + a$, para algum inteiro t, e da segunda, por substituição de x, $nt + a \equiv b \ mod \ m$ que dá $nt \equiv (b - a) \ mod \ m$. Como $mdc(m, n) = 1$, $\bar{n}$ tem inverso em $\mathbb{Z}_m$ e, então, chamando de $\bar{\imath}$ o tal inverso, a solução da congruência é $t \equiv (i\ (b - a)) \ mod \ m$. Portanto, $t = mu + i(b - a)$, com u inteiro. Daí, substituindo em $x = nt + a$, temos $x = nmu + ni(b - a) + a$ ou $x = (1 - ni)a + nib + nmu$. Agora, como $\bar{n}.\bar{\imath} = \bar{1}$ em $\mathbb{Z}_m$, existe um inteiro j tal que $1 - ni = mj$ e, então, $x = mja + nib + nmu$, com u inteiro, é solução do sistema.

Agora, se x_0 e y_0 são duas soluções do sistema, então $x_0 \equiv a \ mod \ n$ e $y_0 \equiv a \ mod \ n$. Daí segue, por transitividade, que $x_0 \equiv y_0 \ mod \ n$ e, assim, $n|(x_0 - y_0)$. *Mutatis mutandis*, $m|(x_0 - y_0)$. Assim, como $mdc(m, n) = 1$, segue da proposição 2.6, $(mn)|(x - y)$ e, então, $x_0 \equiv y_0 \ mod \ (mn)$ e o sistema tem uma única solução em $\mathbb{Z}_{mn}$.

No exemplo

$$x \equiv 1 \ mod \ 11,$$

$$x \equiv 2 \ mod \ 13,$$

temos $x = 13j\times1 + 11i\times2 + 11\times13u = 13j + 22i + 143u$. Como $1 – 11i = 13j$, é fácil determinar, pelo algoritmo de Euclides, valores para i e j. No caso, temos $i = 6$ e $j = -5$ e, assim, $x = 67 + 143u$ é solução do sistema para todo inteiro u. Tomando $u = 0$ temos que $x = 67$ é a única solução módulo $13\times11 = 143$.

Observe que a demonstração do teorema do resto chinês fornece um algoritmo (*algoritmo do resto chinês*) para a solução de um sistema de congruências.

Dados os inteiros positivos m e n, uma *matriz de inteiros de ordem* $m\times n$ é a imagem de uma função f de $\mathbb{Z}_m x \mathbb{Z}_n$ em $\mathbb{Z}$, sendo indicada por $M = (a_{ij})_{m\times n}$, onde $a_{ij} = f(i, j)$ é a imagem do par $(i, j) \in I_m\times I_n$,. O natural m é chamado *número de linhas* e o natural n é o *número de colunas*. Normalmente, uma matriz é exibida com os seus elementos dispostos em uma tabela (no sentido usual do termo) na qual a imagem do par (i, j) ocupa a célula da linha i e da coluna j. Por exemplo, a matriz $M = (a_{ij})_{4x3}$ dada por $a_{ij} = i + j$ pode ser exibida da seguinte forma

$$\begin{pmatrix} 2 & 3 & 4 \\ 3 & 4 & 5 \\ 4 & 5 & 5 \\ 5 & 6 & 7 \end{pmatrix}$$

pois, $a_{11} = 1 + 1$, $a_{12} = 1 + 2 = 3$, $a_{13} = 1 + 3 = 4$, $a_{21} = 2 + 1 = 3$ ...

O Teorema do Resto Chinês tem uma interpretação na forma de uma matriz $M = (a_{ij})_{m\times n}$, com $mdc(m, n) = 1$. O que o Teorema do

Resto Chinês afirma é que podemos construir uma matriz definindo a_{ij}, para $i = 1, 2, ..., m$ e $j = 1, 2, ..., n$, como sendo o inteiro x tal que $1 \leq x \leq mn$, $x \equiv i \ mod \ m$ e $x \equiv j \ mod \ n$ e que, nesse caso, todos os elementos de M são distintos.

7.9 O Teorema de Euler

No capítulo anterior, estudamos o Pequeno Teorema de Fermat, que afirma que se p é primo e p e a são primos ente si, então $p|(a^{p-1} - 1)$ (ou $a^{p-1} \equiv 1 \ mod \ p$, na linguagem das congruências). É muito fácil encontrar um contraexemplo que mostra que a primalidade de p é crucial para a veracidade da afirmação: o leitor pode verificar que a afirmação não é verdadeira para $p = 6$ e $a = 5$.

Leonhard Euler (1707-1783), matemático suíço, encontrou, através de uma mudança no expoente, uma forma de eliminar a exigência da primalidade de p. Para tal, ele concebeu uma função, que ficou denominada *função φ de Euler*, relacionada com o número de elementos inversíveis de $\mathbb{Z}_n$. O teorema advindo dessa modificação ficou conhecido como *Teorema de Euler*, proposição matemática que teve um impacto fenomenal no nosso dia a dia, já que ela é a base do Sistema de Criptografia RSA, que será estudada no capítulo seguinte.

Na proposição 7.7, vimos que um elemento a de $\mathbb{Z}_n$ é inversível se e somente se $mdc(a, n) = 1$. Naturalmente, o número de

elementos de $\mathbb{Z}_n$ que são primos em relação a n fornecerá o número de elementos inversíveis de $\mathbb{Z}_n$. A *função* φ *de Euler* é a função que associa a cada inteiro positivo $n > 1$ o número de elementos inversíveis de $\mathbb{Z}_n$. Por exemplo, $\varphi(2) = 1$, $\varphi(3) = 2$ e $\varphi(4) = 2$, valores estes tirados da observação das tabelas da multiplicação de $\mathbb{Z}_2$, $\mathbb{Z}_3$ e $\mathbb{Z}_4$, apresentadas na seção 7.6. Já $\varphi(12) = 4$, valor tirado da tabela da multiplicação em I_{12} apresentada no capítulo 3.

Na verdade, podemos estabelecer uma fórmula para $\varphi(n)$, como mostra a seguinte proposição.

Proposição 8.7

Sobre a função φ de Euler são verdadeiras as seguintes afirmações:

a) $\varphi(p) = p - 1$ se e somente se p é primo.

b) Se p é primo e n é um inteiro positivo, então $\varphi(p^n) = (p - 1)p^{n-1}$.

c) Se $mdc(m, n) = 1$, então $\varphi(m \cdot n) = \varphi(m)\varphi(n)$.

d) Se $p_1^{e_1}.....p_k^{e_k}$ é a decomposição em fatores primos de um inteiro positivo z, então $\varphi(z) = p_1^{e_1-1}...p_k^{e_k-1}(p_1 - 1)...(p_k - 1)$

Demonstração

a) Se $\varphi(p) = p - 1$, então $\overline{1}, \overline{2}, ..., \overline{p-1}$ são inversíveis e,

portanto, para todo $1 < i < p$, $mdc(p, i) = 1$. Isso mostra que p não tem divisores diferentes de 1 e de p e, por conseguinte, p é primo.

A recíproca decorre de imediato do corolário 4.7.

b) Seja $k = p^n$. O corolário 5.7 afirma que os elementos não inversíveis de $\mathbb{Z}_k$ são p, $2p$, $3p$, ..., $p^{n-1}p$ e, portanto, existem p^{n-1} elementos de $\mathbb{Z}_k$ não inversíveis. Daí, $\varphi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1)$, como queríamos demonstrar.

c) Seja $M = (a_{ij})_{mxn}$ definida, para $i = 0, 1, ..., m-1$ e $j = 0, 1, ..., n-1$, por $a_{ij} = x$ tal que $0 \leq x \leq mn - 1$, $x \equiv i \ mod \ m$ e $x \equiv j \ mod \ n$. Pelo Teorema do Resto Chinês, a matriz M está bem definida e todos os seus elementos são distintos. Seja $x = a_{ij}$. Se $\bar{x}$ tem inverso em $\mathbb{Z}_{mn}$, então existe k tal que $(xk) \equiv 1 \ mod \ (mn)$ o que implica, pela proposição 4.7, $(xk) \equiv 1 \ mod \ m$. Daí, multiplicando $x \equiv i \ mod \ m$ por k e aplicando a transitividade, temos que $(ik) \equiv 1 \ mod \ m$ e, então, $\bar{\imath}$ é inversível em $\mathbb{Z}_m$. Da mesma maneira se prova que se $\bar{x}$ é inversível em $\mathbb{Z}_{mn}$, então $\bar{\jmath}$ é inversível em $\mathbb{Z}_n$.

Reciprocamente, suponhamos que $x = a_{ij}$ e $\bar{\imath}$ e $\bar{\jmath}$ são inversíveis em $\mathbb{Z}_m$ e em $\mathbb{Z}_n$, respectivamente. Sejam $\bar{\imath}'$ o inverso de $\bar{\imath}$ em $\mathbb{Z}_m$ e $\bar{\jmath}'$ o inverso de $\bar{\jmath}$ em $\mathbb{Z}_n$. Pelo Teorema do Resto Chinês existe um inteiro y tal que $0 \leq y \leq mn - 1$ com $y \equiv i' \ mod \ m$ e $y \equiv j' \ mod \ n$. Daí, segue que $(xy) \equiv (ii') \ mod \ m \equiv 1 \ mod \ m$, congruência advinda do fato de que $\bar{\imath}'$ é o inverso de $\bar{\imath}$ em $\mathbb{Z}_m$. Segue então que $m|(xy - 1)$. Com raciocínio

idêntico, prova-se que $n|(xy - 1)$. Assim, pela proposição 2.6, $(mn)|(xy - 1)$, o que prova que $(xy) \equiv 1 \ mod \ (mn)$ e que $\bar{x}$ é inversível em $\mathbb{Z}_{mn}$.

Provamos então que se $x = a_{ij}$ então $\bar{x}$ é inversível em $\mathbb{Z}_{mn}$ se e somente se $\bar{\imath}$ é inversível em $\mathbb{Z}_m$ e $\bar{\jmath}$ o é em $\mathbb{Z}_n$. Daí, $\varphi(mn) = \varphi(m)\varphi(n)$, pois $\varphi(mn)$ é o número de elementos inversíveis de $\mathbb{Z}_{mn}$, $\varphi(m)$ é o número de elementos inversíveis de $\mathbb{Z}_m$ e $\varphi(n)$ é o número de elementos de $\mathbb{Z}_n$.

d) Segue de imediato do item (c) e da fórmula para $\varphi(p^n)$ com p primo.

Por exemplo,

$$\varphi(504) = \varphi(2^3 \times 3^2 \times 7)$$

$$\varphi(504) = 2^2 \times 3^1 \times 7^0 \times (2 - 1) \times (3 - 1) \times (7 - 1)$$

$$\varphi(504) = 4 \times 3 \times 1 \times 1 \times 2 \times 6 = 144.$$

Para demonstrarmos o Teorema de Euler, precisamos da seguinte definição.

Seja n um inteiro maior que 1. O conjunto de inteiros $S = \{a_1, a_2, ..., a_{\varphi(n)}\}$ é dito um *sistema reduzido de resíduos módulo* n se $\overline{a_1}, \overline{a_2}, ..., \overline{a_{\varphi(n)}}$ são os elementos inversíveis de $\mathbb{Z}_n$. Por exemplo, $S = \{1, 17, 59, 67\}$ é um sistema reduzido de resíduos módulo 12, pois, módulo 12, 17 = 5, 59 = 11 e 67 = 7.

Lema 1.7

Seja $S = \{a_1, a_2, ..., a_{\varphi(n)}\}$ um sistema reduzido de resíduos módulo n. Se a é um inteiro tal que $mdc(a, n) = 1$, então $C = \{aa_1, aa_2, ..., aa_{\varphi(n)}\}$ também é um sistema reduzido de resíduos módulo n.

Demonstração

Inicialmente, precisamos mostrar que, de fato, $|C| = |S| = \varphi(n)$. Isto não aconteceria se existissem dois inteiros positivos i e j, menores que $\varphi(n)$ e distintos, tais que $\overline{a \,.\, a_i} = \overline{a \,.\, a_j}$. Porém, se isso acontecesse, teríamos $\bar{a} \,.\, \overline{a_i} = \bar{a} \,.\, \overline{a_j}$, o que implicaria $\overline{a_i} = \overline{a_j}$, pois, como $mdc(a, n) = 1$, $\bar{a}$ é inversível em $\mathbb{Z}_n$. Porém, $\overline{a_i} = \overline{a_j}$ não pode acontecer porque i e j são menores que n. Falta mostrar que $\overline{a \,.\, a_i}$ é inversível para todo i. Mas isso é imediato, pois $\overline{a \,.\, a_i} \,.\, (\overline{a})^{-1} . (\overline{a_i})^{-1} = \bar{a} \,.\, \overline{a_i} \,.\, (\overline{a})^{-1} . (\overline{a_i})^{-1} = \bar{1}$

Teorema 3.7 (*Teorema de Euler*)

Sejam a e n inteiros, com n maior que 1 e $mdc(a, n) = 1$. Então $a^{\varphi(n)} \equiv 1 \ mod \ n$.

Demonstração

Se $S = \{a_1, a_2, ..., a_{\varphi(n)}\}$ é um sistema reduzido de resíduos módulo n, então, pelo lema acima, o conjunto $C = \{aa_1, aa_2, ..., aa_{\varphi(n)}\}$ também o é, já que uma das nossas hipóteses é que

$mdc(a,\ n) = 1$. Então $\overline{a_1}.\overline{a_2}.....\overline{a_n} = \overline{a.a_1}.\overline{a.a_2}.....\overline{a.a_{\varphi(n)}}$, que dá $(a\ .\ a_1\ .\ a\ .\ a_2\ .\ ...\ .\ a\ .\ a_{\varphi(n)}) \equiv (a_1\ .\ a_2\ .\ ...\ .\ a_{\Phi(n)})\ mod\ n$.

Daí, aplicando sucessivamente a lei do cancelamento para congruências (o que pode ser feito, pois $mdc(a_i,\ n) = 1$), temos $a^{\varphi(n)} \equiv 1\ mod\ n$, como queríamos demonstrar.

7.10 Exercícios

Para receber propostas de soluções, basta enviar e-mail para jaime@ic.ufal.br com as seguintes informações: nome completo, categoria (discente/docente), curso, instituição, estado/cidade.

7.0. Podendo se inspirar nos comentários do final da seção 7.2, encontre a solução (u, v) da equação diofantina $x - y = 7$ tal que u e v são potências maiores que 1 de 2 e de 3, respectivamente.

7.0'. Mostre que são iguais os algarismos da casa das unidades de n^5 e n, qualquer que seja o inteiro positivo n.

7.1. Sejam n, u e v inteiros maiores que 1, $d = mdc(u, v)$ e a um inteiro qualquer. Prove que se $a^u \equiv 1\ mod\ n$ e $a^v \equiv 1\ mod\ n$, então $a^d \equiv 1\ mod\ n$.

7.2. Mostre que se $\bar{\imath} = \bar{\jmath}$ em $\mathbb{Z}_n$, então $mdc(i, n) = mdc(j, n)$.

7.3. Mostre que adição $\bar{a} + \bar{b} = \overline{a+b}$ não está bem definida

para a relação de equivalência *a ≈ b se e somente se a e b possuem o mesmo número de divisores primos*.

7.4. Pelo teorema 1.7, temos que se $\bar{a} \in \mathbb{Z}_n$, então -($\bar{a}$) = $\overline{n-a}$. Mostre que $\overline{-a}$ = -($\bar{a}$) = $\overline{n-a}$.

7.5. Mostre que em $\mathbb{Z}_n$ $\overline{n-1}$ é sempre inversível com $\left(\overline{n-1}\right)^{-1} = \overline{n-1}$.

7.6. Mostre que se *p* é primo, 0 < *a* < *p,* e $(\bar{a})^{-1} = (\bar{a})$ em $\mathbb{Z}_p$, então *a* = 1 ou *a* = *p* - 1.

7.7. Utilizando o conceito de classes residuais, apresente uma outra demonstração do *Pequeno Teorema de Fermat* (aqui escrito na linguagem de congruências), já discutido no capítulo anterior:

Se *p* é um número primo e *a* é um inteiro primo em relação a *p*, então $a^{p-1} \equiv 1 \ mod\ p$.

7.8. Apresente um contraexemplo para mostrar que *mdc*(*a*, *n*) = 1 não implica $a^{n-1} \equiv 1 \ mod\ n$.

7.9. Prove o teorema de Wilson: se *p* é um número primo, então (*p* - 1)! ≡ (-1) *mod p*

7.10. (Considerando conhecidos os números racionais, que serão estudados no capítulo 10, e o conceito de probabilidade). Sejam *n* um inteiro tal que *n* = *pq*, com *p* e *q* primos e *z* um número inteiro aleatoriamente escolhido. Prove que a probabilidade de que $\bar{z}$ não seja inversível em $\mathbb{Z}_n$ é $\frac{1}{p} + \frac{1}{q} - \frac{1}{p.q}$.

Mostre que se p e q possuem mais de 30 algarismos, essa probabilidade é menor que 10^{-29} (considerando conhecidos os números reais).

7.11. Determine, se existirem:

a) o inverso de 25 em $\mathbb{Z}_{626}$.

b) o inverso de 21 em $\mathbb{Z}_{80}$.

7.12. Resolva *as* seguintes congruências lineares.

a) $5x + 7 \equiv 10 \ mod\ 15$.

b) $3x - 4 \equiv 0 \ mod\ 4$

7.13. Determine o menor inteiro positivo múltiplo de 9 que deixa resto igual a 1 quando dividido por 2, por 5 e por 7.

7.14. Determine o menor inteiro positivo que deixa restos iguais a 2, 3 e 4 quando dividido, respectivamente, por 3, 5 e 7.

7.15. Determine

a) $\varphi(625)$

b) $\varphi(8!)$

c) $\varphi(5900)$

8 Uma aplicação: o sistema de criptografia RSA

8.1 Introdução

A *criptografia* pode ser entendida como a ação de reescrever um texto de modo que apenas as pessoas autorizadas pelo autor do texto sejam capazes de compreendê-lo. Chamaremos o texto de *mensagem*, a pessoa autorizada a ler a mensagem de *destinatário* e o autor da mensagem de *remetente*. A ação de criptografar uma mensagem será chamada de *codificação* da mensagem.

Historicamente, a criptografia surgiu para envio de mensagens de estratégias de combate em guerras e já era utilizada por Júlio César para envio de mensagens aos seus exércitos em luta na Europa de antes de Cristo. Atualmente, a criptografia é fundamental para a realização de transações comerciais e bancárias na internet.

Utiliza-se a expressão *decodificar* para o ato - que deve ser realizado pelo destinatário - da conversão da mensagem criptografada para a mensagem original, enquanto a expressão *decifrar* é utilizada para a conversão realizada por uma pessoa não autorizada pelo remetente. Em alguns processos de criptografia, se um não destinatário decifra uma mensagem codificada por algum método ele

é capaz de decifrar qualquer mensagem codificada pelo tal método. Dizemos então que o "código foi quebrado", código aí sendo utilizado no sentido do método utilizado para a codificação.

Provavelmente, o primeiro método utilizado para codificação de mensagens tenha sido o de trocar cada letra pela letra seguinte. Como esse método foi facilmente quebrado, introduziu-se o conceito de *chave*: o conjunto dos destinatários recebia previamente um valor inteiro positivo que indicava quanto cada letra deveria ser "transladada" dentro do alfabeto, considerando-o um anel. Por exemplo, se a chave fosse $n = 3$, a mensagem "DEZ HORAS" seria codificada para "GHC LRUDV".

Métodos que consistam simplesmente na substituição de letras por outras (ou por outros símbolos) são relativamente fáceis de serem quebrados em função de que, em qualquer língua, há prevalência de determinados tipos de letra e de combinações das letras. Por exemplo, na nossa língua portuguesa, as vogais são mais frequentes que as consoantes e, entre aquelas, a letra mais frequente é a letra A.

Para dificultar a análise acima, foi introduzido método da "translação variável", no qual cada letra era transladada de acordo com a sua posição no texto e com a posição no alfabeto das letras de uma palavra, que agora seria a *chave* do sistema. Por exemplo, se a chave fosse "MACEIÓ", a primeira letra da mensagem seria transladada 13 posições (13 é a posição da letra M no alfabeto), a

segunda letra da mensagem seria transladada uma posição (letra A) e, assim, sucessivamente. Com a chave MACEIÓ, a mensagem "DEZ HORAS" seria codificada para "QFC MXGNT"

Mesmo levando em conta o fato de que as chaves dos exemplos anteriores eram modificadas periodicamente, a decifração de uma mensagem através da análise estatística das letras permitia a descoberta do método utilizado e da chave atual. A partir daí, todo o sistema estava momentaneamente vulnerável.

Observe que nos dois métodos exemplificados, o conhecimento das chaves para codificação tinha de ser restrito aos possíveis destinatários, implicando mais uma dificuldade: a chave não poderia cair nas mãos do "inimigo". Além disso, as chaves de decodificação são óbvias a partir das chaves de codificação. Por essas razões, estes métodos são chamados *sistemas de criptografia de chave privada* ou *sistemas de criptografia de chaves simétricas*.

Muito se procurou um sistema de criptografia de *chave pública e assimétrica*, no qual, além do método para codificar, as chaves de codificação dos usuários fossem conhecidas de todos.

8.2 O sistema de criptografia RSA

O *sistema de criptografia RSA* é um sistema de criptografia de chave pública, desenvolvido em 1978 por R. L. **R**ivest, A. **S**hamir e

L. **A**dleman, pesquisadores, na época, do Massachussetts Institute of Technology (MIT). A seguir, descreveremos o sistema RSA, mostrando que nele é aplicada toda (quase toda, por precaução) a Matemática desenvolvida neste e nos capítulos anteriores.

Chave de codificação

Cada usuário define uma *chave de codificação* para que um remetente lhe envie mensagens. A chave de codificação consiste em um par de inteiros (n, c) onde n é o produto de dois primos p e q e c é primo em relação a $\varphi(n)$. Vale lembrar que, se $n = pq$ e p e q são primos, então, pelo Teorema Fundamental da Aritmética, p e q são os dois *únicos* fatores de n. Além disto, pela proposição 7.7, $\varphi(n) = \varphi(pq) = \varphi(p)\varphi(q) = (p - 1)(q - 1)$.

O usuário divulga o par (n, c) e guarda, bem guardado, os primos p e q, pois eles são o segredo da *chave de decodificação*.

Chave de decodificação

A partir dos primos p e q, cada usuário determina a sua *chave de decodificação*: par (n, d), onde d é o inteiro menor que $\varphi(n)$ tal que $\bar{d}$ é o inverso de $\bar{c}$ em $\mathbb{Z}_{\varphi(n)}$. Observe que d existe, pois c foi escolhido de tal forma que $\text{mdc}(c, \varphi(n)) = 1$. Quando útil, nos referimos a chave de decodificação como sendo simplesmente a componente d.

Para uma chave segura, deve se escolher dois primos muito grandes com uma razoável diferença entre eles. A segurança da chave

reside no fato, comentado no capítulo anterior, de que não existe algoritmo eficiente para se encontrar um fator primo de números grandes, se o número não possui apenas dois fatores com pequena diferença entre eles. Esse fato implica a quase impossibilidade de se determinar p e q a partir de n.

Exemplos

Para um primeiro exemplo, consideremos os primos $p = 97$ e $q = 53$. Temos:

$n = 97 \times 53 = 5.141$,

$\varphi(n) = (97 - 1) \times (53 - 1) = 4.992$,

$c = 7$ (podemos escolher $c = 7$, pois 7 é primo em relação a 4.992)

Assim, (5.141, 7) é uma chave de codificação válida. Para essa chave de codificação, a chave de decodificação é assim obtida. Como

4.992	7	1
	713	

temos $1 = 4.992 + 7 \times (-713)$, o que implica $d = 7^{-1} = 4\ 992 - 713 = = 4\ 279$. Dessa forma, a chave de decodificação é (5.141, 4.279).

Para um outro exemplo, consideremos os primos $p = 127$ e $q = 193$. Temos:

$n = 127 \times 193 = 24.511$,

$\varphi(n) = 126 \times 192 = 24.192$,

$c = 5$ (5 e 24.192 são primos entre si).

Dessa forma, (24.511, 5) é uma chave de codificação, com chave de decodificação assim determinada:

24 192	5	2	1
	4 838	2	

$1 = 5 - 2\times2 = 5 - (24.192 - 5\times4.838)\times2,$

$1 = (-2)\times24.192 + 5\times9\,677,$

$d = 9.677.$

Conversão da mensagem em um inteiro (*pré-codificação da mensagem*)

Como a *função de codificação* (que será vista a seguir) será definida no conjunto dos inteiros positivos, é necessário que os caracteres da mensagem sejam convertidos em números inteiros. Ou seja, o sistema de codificação deve adotar uma função que faça essa conversão. Adotaremos a função $f(x) = \text{Ascii}(x) + 100$. Para que o leitor possa acompanhar o exemplo discutido a seguir, apresentamos a seguir os valores do código ASCII para as letras maiúsculas do nosso alfabeto.

Letra	A	B	C	*D*	E	F	G	H	*I*	J	K	L	M	N	O
ASCII	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79

Letra	P	Q	R	S	T	U	G	V	Y	X	Z	Espaço
ASCII	65	66	67	68	69	70	71	72	73	74	75	32

Por exemplo, a mensagem I LOVE YOU seria pré-codificada para 173132176179186169132189179185.

Quebra da mensagem ascii-codificada em blocos

Se a mensagem deve ser enviada para o usuário de chave (n, c), o próximo passo para a codificação é quebrar a mensagem ascii-codificada em blocos B_i que correspondam a números inteiros menores do que e primos em relação a n. Como esses números serão objetos de uma função, os blocos B_i não devem começar por zero.

Vale observar que se for encontrado um bloco B_i tal que $\text{mdc}(B_i, n) \neq 1$, teremos que $\text{mdc}(n, B_i) = p$ ou $\text{mdc}(n, B_i) = q$ já que $n = pq$ e p e q são primos. Neste caso, p e q foram encontrados e a chave de decodificação da destinatária foi quebrada. Como mostra o exercício 7.8, quando n tem mais de 30 algarismos, a probabilidade de se encontrar um bloco B_i tal que $\text{mdc}(B_i, n) \neq 1$ é próximo de zero.

Funções de codificação e de decodificação

A codificação de cada bloco é feita através da *função de codificação*, definida de $\mathbb{N}$ em $\mathbb{Z}$ por $Cod(B_i) = (B_i)^c \ mod\ n$, onde (n, c) é a chave de codificação do destinatário. Após a aplicação da função a cada bloco, a mensagem é enviada na forma $M_1\#M_2\#M_3\# \ldots \#M_k$, onde $M_i = Cod(B_i)$ e # é um *separador* adotado para todo o sistema.

A decodificação é realizada pela *função de decodificação*, definida de $\mathbb{N}$ em $\mathbb{Z}$ por $Dec(M_i) = (M_i)^d \ \ mod\ n$, onde d é a chave de decodificação.

Naturalmente, para que o destinatário, após a aplicação da

função de decodificação, tenha acesso à mensagem original, deve-se ter $Dec(M_i) = Dec(Cod(B_i)) = B_i$, o que é garantido pelo seguinte teorema.

Teorema 4.7

Nas condições fixadas acima, se z é um inteiro positivo menor n tal que mdc(z, n) = 1, então $Dec(Cod(z)) = z$.

Demonstração

Inicialmente, observemos que, como $\bar{d}$ é o inverso de $\bar{e}$ em $\mathbb{Z}_{\varphi(n)}$, temos que $ed = k\varphi(n) + 1$, para algum inteiro k. Assim,

$$Dec(Cod(z)) = Dec(z^e \ mod \ n),$$

$$Dec(Cod(z)) = (z^e)^d \ mod \ n,$$

$$Dec(Cod(z)) = z^{ed} \ mod \ n,$$

$$Dec(Cod(z)) = z^{k\varphi(n)+1} \ mod \ n,$$

$Dec(Cod(z)) = (z \ (z^{\varphi(n)})^k) \ mod \ n = z \ mod \ n = z$, pois, como mdc($n$, z) = 1, o Teorema de Euler estabelece que $z^{\varphi(n)} \equiv 1. \ mod \ n$.

Exemplos

Para se enviar a mensagem I LOVE YOU para a usuária de chave (5.141, 7), realizaríamos as seguintes ações:

1. Pré-codificação da mensagem: 173132176179186 169132189179185.

2. Quebra da mensagem pré-codificada em blocos:

$B_1 = 173$

$B_2 = 1321,$

$B_3 = 761$

$B_4 = 79$

$B_5 = 1861$

$B_6 = 691$

$B_7 = 3218$

$B_8 = 917$

$B_9 = 91$

$B_{10} = 85$

3. Verificação de que mdc(B_i, n) =1, para i = 1, 2, 3, …, 10, o que pode ser constatado facilmente pelo leitor.

4. Aplicação da função de codificação

$Cod(173) = 173^7 \ mod\ 5\ 141 = 3288$

$Cod(1321) = 1321^7 \ mod\ 5\ 141 = 417$

$Cod(761) = 761^7 \ mod\ 5\ 141 = 2730$

$Cod(79) = 79^7 \ mod\ 5\ 141 = 3616$

$Cod(1861) = 1861^7 \ mod\ 5\ 141 = 361$

$Cod(691) = 691^7 \ mod\ 5141 = 2142$

$Cod(3218) = 3218^7 \ mod\ 5\ 141 = 1707,$

$Cod(917) = 917^7 \ mod\ 5141 = 579,$

$Cod(91) = 91^7 \ mod\ 5\ 141 = 2237,$

$Cod(85) = 85^7 \ mod\ 5\ 141 = 283,$

Dessa forma, a mensagem a ser enviada à destinatária seria 3288#417#2730#3616#361#2142#1707#597#2237#283.

Para um exemplo de decodificação, imagine que a destinatária de chave de decodificação (2117, 1613) receba a mensagem 815#297#2067#2091#35#659#506#65. Temos

$$Dec(815) = 815^{1\,613} \; mod \; 2117 = 1771$$

$$Dec(297) = 297^{1\,613} \; mod \; 2117 = 691$$

$$Dec(2\,067) = 2067^{1\,613} \; mod \; 2117 = 851$$

$$Dec(2\,091) = 2091^{1\,613} \; mod \; 2117 = 321$$

$$Dec(35) = 35^{1\,613} \; mod \; 2117 = 651$$

$$Dec(659) = 659^{1\,613} \; mod \; 2117 = 77$$

$$Dec(506) = 506^{1\,613} \; mod \; 2117 = 1791$$

$$Dec(65) = 65^{1\,613} \; mod \; 2117 = 82$$

Assim, a mensagem é

177169**185**132**165**1**77179**182

M E **U** **A** M **O** R

Vale observar que os cálculos acima, aparentemente astronômicos, foram realizados por calculadoras instaladas em computadores.

8.3 Exercícios

Para receber propostas de soluções, basta enviar e-mail para jaime@ic.ufal.br com as seguintes informações: nome completo, categoria (discente/docente), curso, instituição, estado/cidade.

8.1. Sabendo que p = 13 e q = 59 são números primos:

a) Encontre um conjunto de chaves pública e privada para um sistema RSA.

b) Codifique a mensagem VOU para o destinatário de chave pública definida no item (a).

8.2. Decifre a mensagem 255#245#66#235 recebida pelo usuário de chave pública (407, 13).

9. Os números inteiros: construção por definição

Tendo compreendido o conceito de classes de equivalências e estando mais maduros em Matemática, estamos aptos a *definir* o conjunto dos inteiros a partir do conjunto dos números naturais $\mathbb{N}$, construído no capítulo 2 através dos axiomas de Peano.

Para tal, definamos a seguinte relação binária no produto cartesiano $\mathbb{N}^2$: $(m, n) \approx (p, q)$ se e somente se $m + q = n + p$. É fácil ver que a relação $\approx$ é de equivalência. De fato, a reflexividade e a simetria são consequências imediatas da reflexividade e da simetria da igualdade e a transitividade é provada da seguinte forma: se $(m, n) \approx (p, q)$ e $(p, q) \approx (t, u)$, então $m + q = n + p$ e $p + t = q + u$ o que implica $m + q + p + t = n + p + q + u$. Daí, $m + t = n + u$ donde se deduz que $(m, n) \approx (t, u)$.

Seja $\mathfrak{Z}$ o conjunto das classes de equivalências da relação $\approx$ e em $\mathfrak{Z}$ definamos as seguintes operações.

i) adição:

$$\overline{(m,\ n)} + \overline{(p,\ q)} = \overline{(m+p,\ n+q)}$$

ii) multiplicação

$$\overline{(m,n)}.\overline{(p,q)} = \overline{(m.q + n.p, m.p + n.q)}$$

Como fizemos para as operações com classes residuais módulo n, necessitamos inicialmente observar que estamos utilizando os mesmos operadores para as operações em $\mathfrak{I}$ e em $\mathbb{N}$ e mostrar que as operações estão bem definidas, no sentido de que somas e produtos independem de particulares representantes das classes. Porém, essa segunda observação é imediata, pois, se $(m', n') \approx (m, n)$ e $(p', q') \approx (p, q)$, para a adição temos $m' + n = n' + m$ e $p' + q = q' + p$, o que implica $(m' + p') + (n + q) = (n' + q') + (m + p)$, acarretando $(m' + p', n' + q') \approx (m + p, n + q)$ e para a multiplicação,

$$q'.(m' + n) = q'.(n' + m),$$
$$p'.(n' + m) = p'.(m' + n),$$
$$n.(p' + q) = n.(q' + p),$$
$$m.(q' + p) = m.(p' + q)$$

o que dá, por adição, $q'.m' + q'.n + p'.n' + p'.m + n.p' + n.q + m.q' + + m.p = q'.n' + q'.m + p'.m' + p'.n + n.q' + n.p + m.p' + m.q$, implicando $m.q' + n'.p' + n.q + m.p = m'.p' + n'.q' + m.q + n.p$, o que mostra que $(m'.q' + n'.p', m'.p', n'.q') \approx (m.q + n.p, m.p + n.q)$.

Proposição 1.8

O conjunto $\mathfrak{I}$ munido das operações definidas acima é um domínio de integridade.

Demonstração

A comutatividade e associatividade da adição e da multiplicação e a distributividade da multiplicação em relação à

adição decorrem de imediato das propriedades das operações em $\mathbb{N}$ e suas verificações serão deixadas como exercício. Também serão deixadas como exercício a verificação das veracidades das seguintes afirmações. Se r é um número natural, a classe de (r, r) é o elemento neutro da adição e a classe de $(r, r+1)$ é o elemento neutro da multiplicação. A classe representada por (n, m) é o elemento simétrico da classe de (m, n).

Agora, omitindo as barras para facilitar, suponhamos que $(m, n).(p, q) = (r, r)$, com $q > p$. Daí, $(mq + np, mp + nq) = (r, r)$ o que implica, nos naturais, $mq + np + r = mp + nq + r$. Daí, utilizando o exercício 2.7, $m(q - p) = n(q - p)$ o que implica, pela lei do corte para os naturais, $m = n$. Logo $(m, n) = (r, r)$.

Do mesmo modo que nos naturais, uma igualdade do tipo $(m, n) + x = (p, q)$ é uma *equação* em $\mathfrak{Z}$ e um elemento (r', r") de $\mathfrak{Z}$ tal que $(m, n) + (r', r") = (p, q)$ é uma *solução* da equação, caso em que dizemos que ela é *solúvel*. Agora, ao contrário dos naturais, toda equação em $\mathfrak{Z}$ é solúvel. De fato, o elemento $(p + n, q + m)$ é tal que $(m, n) + (p + n, q + m) = (p + m + n, q + m + n) = (p, q)$.

Mostraremos agora que podemos definir uma relação de ordem $\mathfrak{Z}$, transformando-o num domínio ordenado.

Proposição 2.8

A relação binária definida em $\mathfrak{Z}$ por $(m, n) \leq (p, q)$ se e somente se $n + p \leq m + q$ em $\mathbb{N}$ é uma relação de ordem compatível com a

adição e com a multiplicação.

Demonstração

Que $(m, n) \leq (m, n)$ é óbvio, pois $m + n = m + n$. Se $(m, n) \leq (p, q)$ e $(p, q) \leq (m, n)$ temos que $n + p \leq m + q$ e $m + q \leq p + n$ o que implica, pela antissimetria de $\leq$ em $\mathbb{N}$, $m + q = n + p$, de onde decorre $(m, n) = (p, q)$. A transitividade e a totalidade de $\leq$ em $\mathfrak{Z}$ são consequências imediatas da transitividade e da totalidade de $\leq$ em $\mathbb{N}$. Para a compatibilidade com a adição, se $(m, n) \leq (p, q)$ temos $n + p \leq m + q$ e então, para todos naturais s e t, $n + p + s + t \leq m + q + s + t$ ou $(n + t) + (p + s) \leq (m + s) + (q + t)$, o que mostra que $(m + s, n + t) \leq (p + s, q + t)$, Daí, $(m, n) + (s, t) \leq (p, q) + (s, t)$. Para a compatibilidade com a multiplicação, se $(m, n) \leq (p, q)$ e $(r, r) \leq (s, t)$, temos $n + p \leq m + q$, $s \leq t$ e $(m, n).(s, t) = (m.t + n.s, m.s + n.t)$, $(p, q).(s, t) = (p.t + q.s, p.s + q.t)$ e $(m.s + n.t) + (p.t + q.s) = (m + q).s + (n + p).t$.

Desta forma, sendo r a raiz da equação $s + x = t$ e t' a raiz da equação $r + x = t$, temos $(m.s + n.t) + (p.t + q.s) = (m + q).r$' $+ (n + p).(s + r)$, o que implica $(m.s + n.t) + (p.t + q.s) = (m + q).(t - r) + (n + p).(s + r)$. Daí, pelo exercício 2.8, $(m.s + n.t) + (p.t + q.s) \leq (m + q).t + (n + p).s$ o que mostra que $(m, n).(s, t) \leq (p, q).(s, t)$.

Proposição 3.8

O conjunto $\mathfrak{I}$ munido das operações e da relação de ordem definidas acima é um domínio bem ordenado.

Demonstração

Sejam os naturais m_0 e n_0 e considere o conjunto $S = \{(m, n) \in \mathfrak{I} | (m, n) > (m_0, n_0)\}$. Temos que $(m_0, n_0 + 1) \in S$. De fato, pelo lema 2.2, $m_0 + n_0 < m_0 + n_0 + 1$ e, portanto, $(m_0, n_0) < (m_0, n_0 + 1)$. Agora, se existisse $(p, q) \in S$ tal que $(p, q) < (m_0, n_0 + 1)$, teríamos $(m_0, n_0) < (p, q) < (m_0, n_0 + 1)$ o que implicaria $n_0 + p < m_0 + q < n_0 + p + 1$, contrariando a proposição 8.2. Logo, $(m_0, n_0 + 1)$ é o elemento mínimo de S.

Dessa forma, o anel $\mathfrak{I}$ é o único domínio bem ordenado, chamado *domínio dos inteiros*, *anel dos inteiros* ou, simplesmente, *conjunto dos inteiros* e é representado por $\mathbb{Z}$. Naturalmente, ficam implícitas, em qualquer denominação, todas as operações, relações e propriedades já estabelecidas ou demonstradas para os domínios bem ordenados.

10. Os números racionais

10.1 Introdução

Os números inteiros não são suficientes para resolver todas as questões do dia a dia. Por exemplo, se uma avó pretende distribuir 25 reais com seus dois netos, não existirá uma quantia inteira de reais que resolva a questão. Ou seja, existem equações do tipo $mx = n$, com m e n inteiros que não são solúveis, como, por exemplo, $2x = 25$ (observe que estamos generalizando, de maneira natural, o conceito de *equação no conjunto dos naturais* discutido no capítulo 2). Neste capítulo, vamos *definir* o conjunto dos *números racionais*, no qual para $m \neq 0$ a equação $mx = n$ é solúvel. Para isto necessitamos definir uma nova estrutura algébrica, chamada *corpo*, cujo conceito, na altura em que estamos, é simples: um *corpo* é um anel no qual todo elemento não nulo é inversível.

O anel dos inteiros não é um corpo, pois os únicos elementos inversíveis dos inteiros são 1 e -1. Já o anel $\mathbb{Z}_5$ é um corpo pois, como para todo inteiro $0 < a < 5$, $mdc(a, 5) = 1$, temos que $\bar{a}$ é inversível em $\mathbb{Z}_5$, qualquer que seja $\bar{a} \in \mathbb{Z}_5$, $\bar{a} \neq \bar{0}$. Por seu turno, $\mathbb{Z}_{12}$ não é um corpo pois, por exemplo, $\bar{6}$ não é inversível. A caracterização dos anéis $\mathbb{Z}_n$ em relação a ser ou não um corpo é muito simples, como

mostra a seguinte proposição.

Proposição 1.10

$\mathbb{Z}_n$ é um corpo se e somente se n é primo.

Demonstração

Se $\mathbb{Z}_n$ é um corpo, então todo elemento $\bar{a}$, não nulo, é inversível e, portanto, pela proposição 7.7, $mdc(a, n) = 1$. Assim, para todo inteiro z, $1 < z < n$, temos que $mdc(z, n) = 1$. Logo n é primo, pois não existe inteiro z, $1 < z < n$ tal que $z|n$.

Reciprocamente, suponhamos que n é primo e seja $\bar{a}$ um elemento não nulo de $\mathbb{Z}_n$. Seja b um representante da classe $\bar{a}$ tal que $1 < b < n$. Com n é primo, temos que $mdc(b, n) = 1$ e, então, pela mesma proposição 7.7, $\bar{b}$ é inversível. Como $\bar{a} = \bar{b}$, temos que $\bar{a}$ é inversível e $\mathbb{Z}_n$ é um corpo.

Lembremos que um anel A é um domínio de integridade se satisfizer a seguinte propriedade: se $a, b \in A$ e $ab = 0$, então $a = 0$ ou $b = 0$. Por exemplo, ainda para lembrar, $\mathbb{Z}_2$ e $\mathbb{Z}_3$ são domínios de integridade, enquanto $\mathbb{Z}_4$ não o é, pois, neste anel, $\bar{2}.\bar{2} = \bar{0}$.

Proposição 2.10

Todo corpo é um domínio de integridade.

Demonstração

Sejam K um corpo e $a, b \in K$ tais que $ab = 0$. Se $a \neq 0$, então existe a^{-1} tal que $a \,.\, a^{-1} = 1$. Assim, multiplicando a igualdade $ab = 0$ por a^{-1}, temos $a^{-1}.(ab) = a^{-1}.0$ o que implica $b = 0$.

10.2 O corpo de frações de um domínio de integridade

Mostraremos agora que um domínio de integridade gera um corpo. Para isso seja A um domínio de integridade e consideremos o conjunto $B = \{(a, b) \in AxA | \ b \neq 0\}$.

Vamos definir em B a relação $(a, b) \approx (a', b')$ se e somente se $a.b' = a'.b$. É fácil ver que $\approx$ é uma relação de equivalência. De fato, a reflexividade decorre da igualdade $a.a = a.a$ e a simetria da igualdade $a'.b = a.b'$. Para a transitividade, suponhamos que $(a, b) \approx (a', b')$ e $(a', b') \approx (a'', b'')$. Devemos provar que $(a, b) \approx (a'', b'')$. De $(a, b) \approx (a', b')$, segue que $a.b' = a'.b$ e de $(a', b') \approx (a'', b'')$, que $a'.b'' = a''.b'$. Multiplicando a primeira dessas igualdades por b'' e a segunda por b, obtemos $a.b'.b'' = a'.b.b''$ e $a'.b''.b = a''.b'.b$, donde se conclui que $a.b'.b'' = a''.b'.b$. Daí, segue que $b'.(a.b'' - a''.b) = 0$ e, portanto, como $b' \neq 0$ e A é um domínio de integridade, $a.b'' = a''.b$, o que prova que $(a, b) \approx (a'', b'')$.

A classe de equivalência de um elemento $(a, b) \in B$, com $b \neq 0$ será indicada por $\frac{a}{b}$ (isto é, $\frac{a}{b} = \{(x, y) \in B | \ (x, y) \approx (a, b)\}$) e o conjunto das classes de equivalência será indicado por K (ou seja, $K = \left\{\frac{a}{b} \mid a, b \in A \text{ e } b \neq 0\right\}$.

Observe que, pela proposição 5.7, $\frac{a}{b} = \frac{c}{d}$ se e somente se $(a, b) \approx (c, d)$, ou seja, se e somente se, $ad = bc$.

Definimos em K as seguintes operações:

Adição: $\frac{a}{b} + \frac{c}{d} = \frac{a.d+b.c}{b.d}$.

Multiplicação: $\frac{a}{b} \times \frac{c}{d} = \frac{a.c}{b.d}$.

Mais uma vez, é necessário que provemos que essas operações estão bem definidas no sentido de que uma soma ou um produto independe do particular representante da classe. Além disso é necessário verificar que toda soma e todo produto são elementos de K. Para isso, basta ver que, como $b \neq 0$, $d \neq 0$ e A é um domínio de integridade, a propriedade (M_4') do capítulo 2 garante que $bd \neq 0$.

Para provar que os resultados independem dos representantes das classes, suponhamos $\frac{a}{b} = \frac{j}{k}$ e $\frac{c}{d} = \frac{m}{n}$. Temos que $ak = bj$ e $cn = dm$, que dão, multiplicando a primeira destas igualdades por dn, $ak'dn = bjdn$ e, multiplicando a segunda por bk, $bkcn = bkdm$ que, somadas, resultam $(ad + bc)kn = (jn + km)bd$ e, portanto, $\frac{a.d+b.c}{b.d} = \frac{j.n+k.m}{k.n}$ o que mostra que $\frac{a}{b} + \frac{c}{d} = \frac{j}{k} + \frac{m}{n}$. Deixamos como exercício mostrar que a multiplicação está bem definida.

Teorema 1.10

Nas condições anteriores e munido das operações definidas acima, K é um corpo, chamado *corpo de frações* do domínio de

integridade *A*.

Demonstração

Temos que provar que *K* é um anel no qual todo elemento não nulo é inversível. A demonstração de que a adição e a multiplicação são associativas e comutativas e que a multiplicação é distributiva em relação à adição são triviais. Por exemplo, levando em conta que $\frac{c}{c} = \frac{1}{1}$, qualquer que seja $c \in A$, $c \neq 0$, a distributividade da multiplicação em relação à soma pode ser demonstrada da seguinte forma.

$$\frac{a}{b} \times \left(\frac{c}{d} + \frac{e}{f}\right) = \frac{a}{b} \times \frac{c.f + d.e}{d.f} = \frac{a.c.f + a.d.e}{b.d.f} \times \frac{b}{b} =$$
$$= \frac{(a.c).(b.f) + (b.d).(a.e)}{(b.d).(b.f)} = \frac{a.c}{b.d} + \frac{a.e}{b.f}$$
$$= \frac{a}{b} \times \frac{c}{d} + \frac{a}{b} \times \frac{e}{f}$$

O elemento neutro da soma é $\frac{0}{1}$, o simétrico de $\frac{a}{b}$ é $\frac{-a}{b}$ (isto é, $-\frac{a}{b} = \frac{-a}{b}$) e o elemento neutro da multiplicação é $\frac{1}{1}$. Falta mostrar que todo elemento tem inverso. Para isto seja $\frac{a}{b}$ não nulo. Então $a \neq 0$ e, por conseguinte, $\frac{b}{a} \in K$. Como $\frac{a}{b} \times \frac{b}{a} = \frac{a.b}{b.a} = \frac{1}{1}$ temos que $\frac{a}{b}$ é inversível e $\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$.

Proposição 3.10

Seja *A* um domínio de integridade e *K* o seu corpo de frações.

Então, para todo $b \in A$, $b \neq 0$,

i) $\frac{a}{-b} = \frac{-a}{b}$

ii) $\frac{-a}{-b} = \frac{a}{b}$

Demonstração

a) Temos $\frac{a}{b} + \frac{a}{-b} = \frac{a.(-b)+b.a}{b.(-b)} = \frac{0}{-b^2} = \frac{0}{1}$ e a igualdade segue.

b) Basta lembrar que a proposição 2.3 garante que $(-a)b = a\,(-b)$.

No exercício 3.4 definimos *subanel* de um anel e solicitamos mostrar que se A e B são anéis e $f : A \to B$ é um homomorfismo, então $f(A)$ é um subanel de B. A próxima proposição mostrará que um domínio de integridade A é isomorfo a um subanel do seu corpo de frações.

Proposição 4.10

Sejam A um domínio de integridade e K o seu corpo de frações. Então a função $j : A \to K$ definida por $j(a) = \frac{a}{1}$ é um homomorfismo injetivo.

Demonstração

Para mostrar que j é um homomorfismo, basta ver que:

i) $j(a + b) = \frac{a+b}{1} = \frac{a}{1} + \frac{b}{1} = j(a) + j(b)$

ii) $j(a \,.\, b) = \frac{a.b}{1} = \frac{a}{1} \times \frac{b}{1} = j(a) \,.\, j(b)$

iii) $j(1) = \frac{1}{1} = 1_K$,

Para mostrar que j é injetivo, suponhamos que $a, b \in A$, com $a \neq b$. Daí, $a \cdot 1 \neq b \cdot 1$ o que implica $\frac{a}{1} \neq \frac{b}{1}$. Logo $j(a) \neq j(b)$ e j é injetivo.

Desse modo, A e $j(A)$ são isomorfos e, portanto, são algebricamente iguais. Isto nos permite identificar $a \in A$ com $\frac{a}{1} \in K$.

10.3 Os números racionais

No ensino fundamental aprendemos que um número racional é todo número que pode ser escrito na forma de uma fração $\frac{p}{q}$ com $q \neq 0$. Naturalmente, essa "definição" não é satisfatória porque não se define anteriormente o que é uma fração nem consegue explicar por que os "números racionais" $\frac{3}{4}$ e $\frac{6}{8}$, por exemplo, são iguais.

A definição formal de números racionais é: o conjunto dos números racionais $\mathbb{Q}$ é o corpo de frações de $\mathbb{Z}$. Assim, um número racional é, formalmente falando, um conjunto, pois é uma classe de equivalência. Por exemplo, $\frac{3}{4} = \left\{\cdots, \frac{-6}{8}, \frac{-3}{4}, \frac{3}{4}, \frac{6}{8}, \frac{9}{12}, \cdots\right\}$

Pela proposição anterior, cada inteiro a pode ser identificado com o racional $\frac{a}{1}$ e podemos então considerar $\mathbb{Z} \subset \mathbb{Q}$. Naturalmente,

se $b|a$, então $\frac{a}{b}$ é inteiro (considerando a identificação), pois $a = bq$, para algum inteiro q, de sorte que $\frac{a}{b} = \frac{bq}{b} = q$. Quando $b \neq 1$, o número racional $\frac{a}{b}$ é chamado *fração*, caso em que a é chamado *numerador* e b é chamado *denominador*.

Da igualdade $\frac{a}{-b} = \frac{-a}{b}$, provada na proposição 4.10, segue que todo número racional pode ser escrito na forma $\frac{a}{b}$ com $b > 0$ e, portanto, todo denominador pode ser considerado positivo.

Além de podermos sempre representar um racional $\frac{a}{b}$ com $b > 0$, podemos sempre representá-lo de tal forma que $mdc(a, b) = 1$, conforme mostra a seguinte proposição.

Proposição 5.10

Seja um racional $\frac{a}{b}$, com $b > 0$. Então existem inteiros j e k tais que $mdc(j, k) = 1$ e $\frac{j}{k} = \frac{a}{b}$.

Demonstração

Seja $d = mdc(a, b)$. Tome, $j = \frac{a}{d}$ e $k = \frac{b}{d}$. Pela observação acima, j e k são inteiros e, pelo exercício 6.4, $mdc(j, k) = 1$. Além disso, $ak = jdk = jb$ e, então, $\frac{j}{k} = \frac{a}{b}$.

Sejam $\frac{a}{b}$ e $\frac{c}{d}$ no corpo $\mathbb{Q}$, com $b > 0$ e $d > 0$. Definimos uma relação binária $\leq$ por $\frac{a}{b} \leq \frac{c}{d}$ se e somente se $ad \leq bc$ em $\boldsymbol{Z}$, onde, por

enquanto, o primeiro ≤ simboliza a relação que estamos definindo e o segundo a relação de ordem em $\mathbb{Z}$. Observe que se $a \leq b$, em $\mathbb{Z}$, temos $a \,.\, 1 \leq b \,.\, 1$, em $\mathbb{Z}$, e, portanto, $\frac{a}{1} \leq \frac{b}{1}$, em $\mathbb{Q}$. Isto significa que se $a \leq b$ em $\mathbb{Z}$ então $a \leq b$ como "elementos" de $\mathbb{Q}$, justificando assim a utilização do mesmo símbolo ≤ para as duas relações.

Proposição 6.10

$\mathbb{Q}$ munido da relação definida acima é um domínio ordenado.

Demonstração

Precisamos mostrar que a relação ≤ é reflexiva, antissimétrica, transitiva, total e é compatível com a adição e com a multiplicação.

Como $ab \leq ba$, em $\mathbb{Z}$, temos que $\frac{a}{b} \leq \frac{a}{b}$, qualquer que seja $\frac{a}{b} \in \mathbb{Q}$, o que mostra a relação é reflexiva. Para a antissimetria, suponhamos que $\frac{a}{b} \leq \frac{c}{d}$ e que $\frac{c}{d} \leq \frac{a}{b}$. Daí, $ad \leq bc$ e $bc \leq ad$, em $\mathbb{Z}$. Como ≤ em $\mathbb{Z}$ é antissimétrica, $bc = ad$ e, portanto, $\frac{a}{b} = \frac{c}{d}$. Para mostrar a transitividade, suponhamos que $\frac{a}{b} \leq \frac{c}{d}$ e $\frac{c}{d} \leq \frac{e}{f}$. Daí, $ad \leq bc$ e $cf \leq de$. Como estamos supondo que $b > 0$ e $f > 0$, temos pela compatibilidade com a multiplicação de ≤ em $\mathbb{Z}$, que $adf \leq bcf$ e $bcf \leq bde$. Daí, pela transitividade de ≤ em $\boldsymbol{Z}$, $adf \leq bd$e. Como $d > 0$, o item (*b*) do exercício 3.7 garante que $af \leq be$, donde se conclui que $\frac{a}{b} \leq \frac{e}{f}$.

Para verificar que ≤ em $\mathbb{Q}$ é total, basta ver que se $\frac{a}{b}$ e $\frac{c}{d}$ são elementos de $\mathbb{Q}$, então, pela totalidade de ≤ em $\mathbb{Z}$, $ad \leq bc$ ou $bc \leq ad$. Daí, $\frac{a}{b} \leq \frac{c}{d}$ ou $\frac{c}{d} \leq \frac{a}{b}$.

As demonstrações de que ≤ é compatível com a adição e com a multiplicação serão deixadas como exercício.

Sendo $\mathbb{Q}$ um domínio ordenado, podemos utilizar todas as propriedades dessa estrutura algébrica obtidas no capítulo 3.

10.4 "Números" não racionais

No corpo dos números racionais toda equação da forma $ax = b$ é solúvel para todo $a \neq 0$. De fato, a, sendo não nulo, possui um inverso a^{-1} e, então, multiplicando a equação por esse inverso, temos $a^{-1}(ax) = a^{-1}b$ e, portanto, $x = a^{-1}b$.

Infelizmente, o corpo dos números racionais ainda não é suficiente para resolver todas as questões de matemática. Por exemplo, como $(-2)^2 = 2^2 = 4$, a equação $x^2 = 4$ tem solução no corpo $\mathbb{Q}$ (identificando o inteiro 2 como o racional $\frac{2}{1}$). Do mesmo modo, a equação $x^2 = \frac{9}{16}$ também tem solução em $\mathbb{Q}$, a saber, $x_1 = \frac{3}{4}$ e $x_2 = -\frac{3}{4}$. A questão é saber se dado qualquer racional $\frac{m}{n}$ existe um racional x tal que $x^2 = \frac{m}{n}$. A resposta negativa a essa pergunta é um

exemplo de que os racionais não bastam para a matemática.

Quando uma equação do tipo $x^2 = \frac{m}{n}$ tem solução, sua solução positiva é indicada por $\sqrt{\frac{m}{n}}$, chamada *raiz quadrada de* $\frac{m}{n}$. Isso significa que $\sqrt{p} = q$ implica $p = q^2$. Por exemplo, $\sqrt{4} = 2$ e $\sqrt{\frac{9}{16}} = \frac{3}{4}$.

A questão é que nem sempre uma raiz quadrada é um número racional como mostra a proposição a seguir.

Proposição 7.10

Se p é um número primo, então $x^2 = p$ não tem solução em $\mathbb{Q}$.

Demonstração

Suponhamos por contradição que $x^2 = p$ tenha solução em $\mathbb{Q}$. Assim, $\sqrt{p} = \frac{m}{n}$, com m e n são primos entre si (ver proposição 5.10), e, então, $p = \frac{m^2}{n^2}$ que dá $m^2 = pn^2$. Daí, $p|m^2$ e, portanto, $p|m$, pois p é primo. Segue então que $m = kp$, para algum inteiro k ou, ainda, $m^2 = k^2p^2$, para algum inteiro k. Substituindo m^2 em $m^2 = pn^2$, temos que $k^2p^2 = pn^2$ e, então, pela lei do cancelamento, $k^2p = n^2$, o que mostra que $p|n^2$, donde segue que $p|n$. Porém essa conclusão é absurda pois, assim, p seria fator comum de m e n que m e n são primos entre si.

10.5 Divisão euclidiana - parte II

Nas primeiras séries do ensino fundamental, somos levados a compreender o quociente de uma divisão euclidiana como sendo *o número de vezes que o divisor está contido no quociente*. Evidentemente, o número de vezes que o divisor está contido no dividendo é o *maior* inteiro que multiplicado pelo divisor resulta um produto menor do que o dividendo. Esse raciocínio justifica, inclusive, o algoritmo que nos é ensinado para efetuar divisões de inteiros. Por exemplo, para dividir 30 por 7 procuramos, por tentativa, o maior inteiro que multiplicado por 7 dá um número menor que 30. Isto pode ser obtido através das multiplicações

$$1\times7 = 7,$$

$$2\times7 = 14,$$

$$3\times7 = 21,$$

$$4\times7 = 28,$$

$$5\times7 = 35,$$

e, portanto, o quociente, é igual a 4, pois $5\times7 > 30$.

Isso sugere o seguinte algoritmo (já discutido no capítulo 5) que, recebendo como entrada dois inteiros positivos m e n fornece como saída o resto e o quociente da divisão euclidiana $m \div n$.

leia(m , n);
  q := 0;

repita enquanto $nq < m$
$q := q + 1$;
$q := q - 1$;
$r := m - nq$;
escreva(q, r);

A parada desse algoritmo é consequência da propriedade arquimediana dos inteiros, discutida no corolário 5.3. Que a saída são o quociente e o resto de $m \div n$ é o que mostraremos a seguir, de uma forma diferente daquela apresentada no capítulo 5.

A função *parte inteira* ou *maior inteiro contido* é a função de $\mathbb{Q}$ em $\mathbb{Z}$, simbolizada por $\lceil\ \rceil$, definida por $\lceil x \rceil = z$, tal que $z \leq x$ e se $m \in \mathbb{Z}$ e $m \leq x$, então $m \leq z$.

Proposição 8.10

Sejam os inteiros m, n, com $n > 0$. Se q é o quociente da divisão euclidiana $m \div n$, então $q = \lceil \frac{m}{n} \rceil$.

Demonstração

Seja $r = r(m, n)$. Assim $0 \leq r < n$ e $m = nq + r$. Multiplicando esta igualdade por $\frac{1}{n}$ obtemos $\frac{m}{n} = q + \frac{r}{q}$ (lembre que $m = \frac{m}{1}$) e, dai, como $n > 0$ e $r \geq 0$, temos $\frac{m}{n} \geq q$. Por outro lado, como de $0 \leq r < n$ segue que $0 \leq \frac{r}{n} < 1$, temos que $\frac{m}{n} < q + 1$. Logo $q \leq \frac{m}{n} < q + 1$, o que mostra que $\lceil \frac{m}{n} \rceil = q$.

Voltando ao algoritmo anterior, observe que a estrutura de

repetição para quando $q = \left\lfloor \frac{m}{n} \right\rfloor + 1$ e a instrução seguinte faz $q = \lceil \frac{m}{n} \rceil$, o que, pela proposição acima, é o quociente procurado. O fato de que o valor de r fornecido pelo algoritmo é o resto da divisão é consequência do teorema da divisão euclidiana.

Para denominador 2 e numerador positivo, temos uma desigualdade simples de ser provada, que será utilizada na próxima seção.

Proposição 9.10

Para todo inteiro positivo m, $\lceil \frac{m}{2} \rceil \geq \frac{m}{2} - \frac{1}{2}$

Demonstração

Se m é par, $m = 2k$, para algum inteiro k, e $\frac{m}{2} = k$. Portanto, $\lceil \frac{m}{2} \rceil = k$. Como, $k \geq \frac{k}{2} - \frac{1}{2}$ a desigualdade segue. Se m é ímpar, $m = 2k + 1$, para algum inteiro k, e $\frac{m}{2} = \frac{2k+1}{2} = k + \frac{1}{2}$. Assim $\lceil \frac{m}{2} \rceil = k$ e a desigualdade segue da mesma forma.

10.6 O algoritmo de Euclides - parte II

Apresentaremos agora uma estimativa para a eficiência do algoritmo de Euclides, medida através do número de iterações necessárias para a obtenção do máximo divisor de dois inteiros positivos dados.

Para isso, consideremos o conjunto $B^2 = \{z \in \mathbb{Z} | z = 2^n$, para algum inteiro $n \geq 0\}$, o conjunto das potências de dois, e a função de $\mathbb{Z}$ em B^2, indicada por $\lfloor z \rfloor_2$ e chamada *função menor potência de dois*, definida por $\lfloor z \rfloor_2 = y$, tal que $y \geq z$ e se $m \in B^2$ e $m \geq z$ então $m \geq y$.

Por exemplo, $\lfloor 5 \rfloor_2 = 8$, $\lfloor -4 \rfloor_2 = 1$, $\lfloor 60 \rfloor_2 = 64$.

Consideremos também a função de B^2 em $\mathbb{Z}$, indicada por lg_2 e chamada *função logarítmica na base dois restrita às potências de dois*, definida por $lg_2\ x = y$ se $x = 2^y$. Por exemplo, $lg_2\ 1 = 0$, pois $1 = 2^0$, $lg_2\ 32 = 5$, pois $2^5 = 32$.

Proposição 10.10

A função logarítmica na base dois restrita às potências de dois é *crescente* no sentido de que se $x, y \in B^2$ e $x > y$, então $lg_2\ x > lg_2\ y$.

Demonstração

Sejam $lg_2\ x = m$ e $lg_2\ y = n$. Então $2^m = x$ e $2^n = y$ e, portanto, $2^m > 2^n$. Daí, pelo exercício 3.16, $m > n$.

Proposição 11.10

Sejam a e b dois inteiros positivos, com $a \geq b$, e n o número de iterações do algoritmo de Euclides no cálculo de $mdc(a, b)$. Então $n < 2\ .\ (1 + lg_2\ \lfloor b \rfloor_2)$.

Demonstração

Do algoritmo de Euclides temos

$$a = b\ .\ q_1 + r_2, \qquad 0 \leq r_2 < b$$

$b = r_2 \,.\, q_2 + r_3, \qquad 0 \le r_3 \le r_2$

$r_2 = r_3 \,.\, q_3 + r_4, \qquad 0 \le r_4 < r_3$

. . . . . .

$r_{n-1} = r_n \,.\, q_n + r_{n+1}, \qquad r_n > 0$ e $r_{n+1} = 0$.

Pondo $r_1 = b$, pela proposição 4.5, temos que, para todo $i = 1, 2, ..., n\text{-}1$, $r_{i+2} < \frac{r_i}{2}$.

Assim, levando em conta o fato de que $r_n \ge 1$, $1 \le r_n < \frac{r_{n-2}}{2} < \frac{r_{n-4}}{2} < ... < \frac{r_{n-\lceil\frac{n-1}{2}\rceil}}{2^{\lceil\frac{n-1}{2}\rceil}} \le \frac{b}{2^{\lceil\frac{n-1}{2}\rceil}}$ e, portanto $2^{\lceil\frac{n-1}{2}\rceil} < b$.

Como, por definição $b \le \lfloor b \rfloor_2$, temos que $2^{\lceil\frac{n-1}{2}\rceil} \le \lfloor b \rfloor_2$ e então, pela proposição anterior, $lg_2\, 2^{\lceil\frac{n-1}{2}\rceil} \le lg_2\, \lfloor b \rfloor_2$. Daí, $\lceil\frac{n-1}{2}\rceil \le lg_2\, \lfloor b \rfloor_b$ e, como $\lceil\frac{n-1}{2}\rceil \ge \frac{n-1}{2} - \frac{1}{2}$, temos $\frac{n-1}{2} - \frac{1}{2} \le lg_2\, \lfloor b \rfloor_2$ donde segue, $n \le 2\,.\,(1 + lg_2\, \lfloor b \rfloor_2)$.

Por exemplo, para se calcular *mdc*(325.678, 125.786) temos $b = 125.786$, $\lfloor 125.786 \rfloor_2 = 131.072$ e $lg_2\, \lfloor 125.786 \rfloor_2 = 17$ e $n < 36$.

Cabe alertar que as funções *maior potência de dois* e *logarítmica restrita às potências de dois* não fazem parte da literatura matemática. Provavelmente, o leitor conhece a função logarítmica definida nos reais e deve estar estranhando a introdução dessas funções. A nossa intenção foi manter a filosofia de só utilizar conceitos estudados previamente (e o conjunto dos reais ainda não o

foi) e dar uma ideia de como pode ser desenvolvida uma pesquisa (com certeza, ingênua) em Matemática, quando novas definições são formuladas em função do que se pretende provar.

10.7 Exercícios

Para receber propostas de soluções, basta enviar e-mail para jaime@ic.ufal.br com as seguintes informações: nome completo, categoria (discente/docente), curso, instituição, estado/cidade.

10.1. (Estudadas na Educação Básica como *propriedades das proporções*) Sejam a, b, c e d números inteiros, com $b \neq 0$ e $d \neq 0$. Mostre que se $\frac{a}{b} = \frac{c}{d}$, então

a) $\frac{a+b}{b} = \frac{c+d}{d}$.

b) $\frac{a+c}{b+d} = \frac{c}{d}$.

c) $\frac{a-b}{b} = \frac{c-d}{d}$.

d) $\frac{a+b}{a-b} = \frac{c+d}{c-d}$, se $a \neq b$ e $c \neq d$.

e) $\frac{a}{c} = \frac{b}{d}$, se $c \neq 0$.

10.4. Enuncie as compatibilidades com a adição e com a multiplicação da relação de ordem definida em $\mathbb{Q}$ e as demonstre.

10.5. (*Propriedade Arquimediana* dos racionais) Sejam

a, $b \in \mathbb{Q}$, com b $\neq 0$. Mostre que existe um inteiro n tal que $n \,.\, b \geq a$.

10.6. Sejam a, $b \in \mathbb{Q}$. Mostre que $a > b > 0$ se e somente se $b^{-1} > a^{-1} > 0$.

10.7. Prove que todo domínio de integridade finito é um corpo.

10.8. Mostre que quaisquer que sejam os racionais r_1 e r_2, com $r_2 \geq r_1$, existe um racional r tal que $r_1 \leq r \leq r_2$.

10.9. Mostre que o conjunto limitado inferiormente $S = \{x \in \mathbb{Q} | \; 0 < x < 1\}$ não tem elemento mínimo, o que mostra que $\mathbb{Q}$ não é um domínio bem ordenado.

11. Os números reais

11.1 Introdução

Desde a Grécia antiga, já se sabia que os racionais não eram suficientes para representar todas as medidas da natureza. Do Teorema de Pitágoras, concluímos que a hipotenusa do triângulo retângulo isósceles com catetos iguais à unidade, tem medida a tal que $a^2 = 2$ e foi mostrado no capítulo anterior que tal número a não é racional. Argumentos igualmente simples permitem mostrar que múltiplos de uma tal medida também não são números racionais. Em outras palavras, não há uma bijeção entre o conjunto $\mathbb{Q}$ e os pontos da reta. Fez-se, portanto, necessária a extensão do conceito de número de tal forma a preencher tais lacunas. Essa extensão deveria, naturalmente, manter as propriedades algébricas satisfeitas pelo corpo $\mathbb{Q}$.

Até o século XIX, os matemáticos trabalharam, e conseguiram grandes avanços, usando o conceito intuitivo do contínuo real. No final daqueles anos, pelo menos três métodos foram usados para a construção dos reais : os *Intervalos Encaixantes*, os *Cortes de Dedekind* e o *Método das Sequencias de Cauchy*, devido a Cantor (Georg Cantor (1845-1918)), que abordaremos aqui por considerá-lo o menos abstrato. A base do processo é caracterizar os “buracos”

existentes por sequências de racionais que, num certo sentido, se acumulam em volta de cada um.

11.2 Sequência de números racionais

O conjunto S(ℚ) das sequências de racionais pode ser facilmente munido da estrutura de anel com as operações $(a_n) + (b_n) = (a_n + b_n)$ e $(a_n) \,.\, (b_n) = (a_n \,.\, b_n)$ e em S(ℚ) alguns subconjuntos se destacam, quer pela natureza dos seus elementos, quer pelas propriedades algébricas dentro do anel. Os dois exemplos a seguir ilustram alguns desses casos.

Exemplo 1. Considere (a_n), onde $a_n = \frac{1}{n}$, $n \in \mathbb{N}$. Para cada $\varepsilon \in \mathbb{Q}$, com $\varepsilon > 0$, existe $n_0 \in \mathbb{N}$ tal que $n_0 > \frac{1}{\varepsilon}$, já que ℚ é arquimediano (exercício 10.4). Assim, se $n > n_0$, $\frac{1}{n} < \in$. Como $0 < \frac{1}{n}$, podemos concluir que para $n > n_0$, $0 < \frac{1}{n} < \varepsilon$. Isso pode ser interpretado da seguinte maneira: a sequência $\frac{1}{n}$ fica tão pequena quanto for exigido, ou que $\frac{1}{n}$ se aproxima de zero quando n cresce.

Exemplo 2. Uma sequência bem conhecida na Matemática do ensino médio é a das somas parciais S_n de uma progressão geométrica (P.G.). Quando uma tal P.G. possui razão $0 < q < 1$, lá dá-se um significado ao que se chama soma infinita, que pode ser representada

por S_∞ e mostra-se que $S_\infty = \frac{a_1}{1-q}$. Essa fórmula decorre da observação de que na fórmula de S_n (ver exercício 3.22), uma das parcelas se comporta de forma semelhante à da sequência do exemplo 1.

Daremos agora a definição que formaliza a ideia contida nos dois exemplos acima. Uma sequência $(a_n) \in S(\mathbb{Q})$ é dita *convergente* para um elemento $a \in \mathbb{Q}$ se, para cada $\varepsilon \in \mathbb{Q}$, com $\varepsilon > 0$, existir $n_0 \in \mathbb{N}$ tal que se $n \geq n_o$, então $|a_n - a| < \varepsilon$. Esse elemento a é chamado *limite da sequência* e escreve-se $lim\ a_n = a$.

Assim, no exemplo 1 a sequência $\frac{1}{n}$ converge para zero, enquanto no exemplo 2, a sequência (S_n) converge para S_∞ ou seja, $lim\ \frac{1}{n} = 0$ e $lim\ S_n = S_\infty$.

Proposição 1.11

Se limite de (a_n) existe, ele é único

Demonstração

Sejam $lim\ a_n = a_1$ e $lim\ a_n = a_2$. Então, para $\varepsilon = \frac{|a_1 - a_2|}{2}$, existem n_o e n'_o tais que se $n \geq n_o$, $|a_n - a_1| < \varepsilon$ e se $n \geq n'_o$, $|a_n - a_2| < \varepsilon$. Tomando $n_1 = max\ \{n_o, n'_o\}$ teremos que se $n \geq n_1$, $|a_1 - a_2| = |a_1 - a_2 + a_n - a_n| \leq |a_1 - a_n| + |a_n - a_2| < 2\varepsilon = |a_1 - a_2|$, o que é uma contradição.

Exemplo 3. A sequência (a_n), onde $a_n = (-1)^n$, não é convergente. Com efeito, suponhamos que (a_n) seja convergente e

seja $lim\ a_n = a$. Se a $\neq 1$, tome $\varepsilon = \frac{|a_1 - 1|}{2}$ e observe que para qualquer n_o, sempre existirão infinitos índices $n > n_o$ tais que $a_n = 1$ e portanto $|a_n - a| = |1 - a| > \frac{|a_1 - 1|}{2}$. Se $a \neq -1$, tome $\varepsilon = \frac{|a_1 - (-1)|}{2}$ e repita a observação. Assim, a deverá ser 1 e –1, mas, devido à unicidade do limite, isto não é possível.

A seguir, enunciamos algumas propriedades das sequências convergentes, facilmente verificáveis. Se $lim\ a_n$ e $lim\ b_n$ existem, então

(a) $lim\ (a_n + b_n) = lim\ (a_n) + lim\ (b_n)$.

(b) $lim\ (k\ .\ a_n) = k\ .\ lim\ (a_n)$, $k \in \mathbb{Q}$.

(c) $lim\ (a_n\ .\ b_n) = lim\ (a_n)\ .\ lim\ (b_n)$

Um outro resultado bastante simples, mas que desempenha um importante papel na construção que faremos, é dado na seguinte proposição.

Proposição 2.11

Se (a_n) é uma sequência constante, isto é, $a_n = a$, então $lim\ a_n = a$.

Demonstração

Para $\varepsilon \in \mathbb{Q}$, com $\varepsilon > 0$, faça $n_0 = 1$. Então, para todo $n_o \geq 1$, $|a_n - a| = |a - a| = 0 < \varepsilon$.

Uma característica das sequências convergentes é uma propriedade intrínseca que elas possuem, não envolvendo o seu limite.

Proposição 3.11

Se (a_n) é uma sequência convergente em $\mathbb{Q}$ então para cada $\varepsilon > 0$, existe $n_o \in \mathbb{N}$ tal que se $n, m \geq n_o$, então $|a_n - a_m| < \varepsilon$.

Demonstração

Seja $(a_n) \in S(\mathbb{Q})$ e $lim\ a_n = a$. Então, se $\varepsilon \in \mathbb{Q}$, com $\varepsilon > 0$, existe $n_o \in \mathbb{N}$ tal que se $n, m \geq n_o$, $|a_n - a| < \frac{\varepsilon}{2}$ e $|a_m - a| < \frac{\varepsilon}{2}$. Logo, $|a_n - a_m| = |a_n - a_m - a + a| \leq |a_n - a| + |a_m - a| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon$.

Essa propriedade motiva a seguinte definição. Uma sequência $(a_n) \in S(\mathbb{Q})$ é dita *de Cauchy* se, para cada $\varepsilon > 0$, existir $n_0 \in \mathbb{N}$ tal que se $n, m \geq n_o$, então $|a_n - a_m| < \varepsilon$.

Tal como foi definida, toda sequência convergente é de Cauchy, mas a recíproca não é verdadeira como mostra o exemplo seguinte.

Exemplo 4. Seja (a_n) tal que $a_o = 0$ e $a_{n+1} = \frac{1}{2 + a_n}$ e suponhamos que $lim\ a_n = a$. Então $lim\ (a_{n+1}) = lim\ (a_n) = lim\ \frac{1}{2 + a_n} = \frac{1}{2 + lim\ a_n}$. Logo, $a = \frac{1}{2 + a}$ o que implica $(a + 1)^2 = 2$, o que não é possível com $a \in \mathbb{Q}$. Isso mostra que (a_n) não é convergente. Por outro lado,

$$|a_{n+1} - a_n| = \left|\frac{1}{2 + a_n} - \frac{1}{2 + a_{n-1}}\right|$$

$$|a_{n+1} - a_n| = \left|\frac{(2 + a_{n-1}) - (2 + a_n)}{(2 + a_n)(2 + a_{n-1})}\right|$$

$$|a_{n+1} - a_n| = \left|\frac{a_{n-1} - a_n}{(2 + a_n)(2 + a_{n-1})}\right|$$

$$|a_{n+1} - a_n| = \left|\frac{a_{n-1} - a_n}{(2+a_n)(2+a_{n-1})}\right|$$

$$|a_{n+1} - a_n| = \frac{1}{4}|a_n - a_{n-1}|$$

e, então,

$$|a_3 - a_2| = \frac{1}{4}|a_2 - a_1|$$

$$|a_3 - a_2| = \frac{1}{4}|a_2 - a_1|$$

$$|a_4 - a_3| = \frac{1}{4}|a_3 - a_2| \leq \left(\frac{1}{4}\right)^2 |a_2 - a_1|$$

...

$$|a_{n+1} - a_n| \leq \left(\frac{1}{4}\right)^{n-1} |a_2 - a_1|$$

e, daí,

$$|a_{n+p} - a_n| = \frac{1}{4}|a_3 - a_2| \leq \left(\frac{1}{4}\right)^2 |a_2 - a_1|$$

$$|a_{n+p} - a_n| \leq |a_{n+p} - a_{n+p-1}| + \ldots |a_{n+1} - a_n|$$

$$|a_{n+p} - a_n| \leq \left(\left(\frac{1}{4}\right)^{n+p-2} + \cdots + \left(\frac{1}{4}\right)^{n-1}\right)|a_2 - a_1|$$

$$|a_{n+p} - a_n| \leq \frac{\left(\frac{1}{4}\right)^{n-1}}{1-\frac{1}{4}}|a_2 - a_1|$$

o que mostra que a sequência (a_n) é de Cauchy, pois é fácil ver que $lim\ \frac{\left(\frac{1}{4}\right)^{n-1}}{1-\frac{1}{4}}|a_2 - a_1| = 0$. (Da penúltima para a última desigualdade, foi utilizada a fórmula dada no exercício 3.22).

O exemplo acima e a proposição 2.11 são dois resultados sobre

os quais a construção dos reais em grande parte se baseia. A ideia é usar as sequências de Cauchy para a construção de elementos de um conjunto e dar a esse conjunto uma estrutura de corpo. Tal conjunto, com um certo abuso de linguagem, conterá os racionais (ver proposição 2.11) e as lacunas existentes em $\mathbb{Q}$ serão preenchidos via sequências do tipo apresentado no exemplo 4.

11.3 Os números reais

No que se segue, denotaremos por $S_o(\mathbb{Q})$ o conjunto das sequências de $S(\mathbb{Q})$ que convergem para zero e por $S_c(\mathbb{Q})$ aquelas que são de Cauchy.

Proposição 4.11

Se $(a_n), (b_n) \in S_o(\mathbb{Q})$, então

i) $(a_n) + (b_n) \in S_0(\mathbb{Q})$,

ii) $(a_n) \,.\, (b_n) \in S_0(\mathbb{Q})$.

Demonstração

Sejam (a_n) e (b_n) tais que $lim\ a_n = 0$ e $lim\ b_n = 0$ e $\varepsilon \in \mathbb{Q}$, com $\varepsilon > 0$.

i) Existem $n_1, n_2 \in \mathbb{N}$ tais se $n \geq n_1$, $|a_n - 0| < \frac{\varepsilon}{2}$ e se $n \geq n_2$, $|b_n - 0| < \frac{\varepsilon}{2}$. Então, se tomarmos $n_0 = max\{n_1, n_2\}$ e $n \geq n_o$, então

$|a_n + b_n - 0| = |a_n + b_n| \leq |a_n| + |b_n| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon$, o que mostra que $(a_n) + (b_n) \in S_0(\mathbb{Q})$.

ii) Existem $n_1 \in \mathbb{N}$ tal que se $n \geq n_1$, então $|a_n| < 1$ e $n_2 \in \mathbb{N}$ tal que se $n \geq n_2$, então $|b_n| < \varepsilon$. Assim, se $n_0 = \max\{n_1, n_2\}$ e $n \geq n_0$, temos $|a_n \,.\, b_n| = |a_n| \,.\, |b_n| < 1 \,.\, \varepsilon = \varepsilon$.

Um fato interessante é que se duas sequências (a_n) e (b_n) em $S(\mathbb{Q})$ convergem para o mesmo racional a, então a sequência $(a_n - b_n) \in S_o(\mathbb{Q})$. Isso resulta imediatamente das propriedades do limite e motiva a seguinte definição. Em $S_c(\mathbb{Q})$ definimos a relação $(a_n) \approx (b_n)$ se $(a_n - b_n) \in S_o(\mathbb{Q})$.

É fácil verificar que essa relação é uma relação de equivalência. Além disso, se (a_n), (b_n) e (c_n) pertencem a $S_c(\mathbb{Q})$ e $(a_n) \approx (b_n)$ temos $(a_n + c_n) - (b_n + c_n) = (a_n - b_n) \in S_o(\mathbb{Q})$ e $(a_n \,.\, c_n) - (b_n \,.\, c_n) = (a_n \,.\, c_n - b_n \,.\, c_n) = (a_n - b_n) \,.\, c_n$. Como $(c_n) \in S_c(\mathbb{Q})$, dado $\varepsilon = 1$, existe n_0 tal que se $m > n_0$, $|c_m - c_{n_0}| < 1$ e, portanto, $|c_m| < 1 + |c_{n_0}|$, se $m > n_0$, o que implica $|c_n| < M$, com $M = max\{|a_1|, \ldots, |a_{n_0}|, |a_{n_0}| + 1\}$, o que permite concluir que $lim\,((a_n - b_n) \,.\, c_n) = 0$, ou seja, $(a_n \,.\, c_n) - (b_n \,.\, c_n) \in S_o(\mathbb{Q})$.

Os resultados que acabamos de verificar mostram que a relação de equivalência obtida também é compatível com as operações de adição e multiplicação. O conjunto das classes de equivalência de $\approx$ será denotado por $\mathbb{R}$ e chamado *conjunto dos*

números reais.

Em $\mathbb{R}$ definimos as operações

i) adição

$$\overline{(a_n)} + \overline{(b_n)} = \overline{(a_n + b_n)}$$

ii) multiplicação

$$\overline{(a_n)}.\overline{(b_n)} = \overline{(a_n.b_n)}$$

que definem uma estrutura de anel em $\mathbb{R}$, fato de fácil verificação. Por exemplo, o elemento neutro da adição é a classe $\overline{(0)}$ da sequência constante (0, 0, ..., 0, ...) e o elemento neutro da multiplicação é a classe $\overline{(1)}$ da sequência constante (1, 1, ..., 1, ...).

A próxima proposição permite concluir que, mais que um anel, $\mathbb{R}$ é um corpo.

Proposição 5.11

Seja $(a_n) \in S_c(\mathbb{Q})$ tal que $(a_n) \notin S_0(\mathbb{Q})$. Então existem um natural n_0 e um racional positivo ε tal que $|a_n| > \varepsilon$, para todo $n \geq n_0$.

Demonstração

Suponha por contradição que o resultado fosse falso. Então para cada racional positivo ε e para todo natural n_0 existiria um natural – que depende do n_0, daí a notação – $m(n_0)$ tal que $m(n_0) \geq n_0$ e $|a_{m(n_0)}| < \frac{\varepsilon}{2}$. Mas, como (a_n) é de Cauchy, existe um natural n_0 tal que $|a_m - a_n| < \frac{\varepsilon}{2}$, se m, $n > n_0$. Assim, para $n > n_0$, teríamos $|a_n| = |a_{m(n_0)} - a_{m(n_0)} + a_n| \leq |a_{m(n_0)} - a_n| + |a_{m(n_0)}| < \varepsilon$ e (a_n)

pertenceria a $S_0(\mathbb{Q})$, o que é uma contradição.

Agora, considere um $a \in \mathbb{R}$, $a \neq 0$. Então $a = \overline{(a_n)}$, com $(a_n) \notin S_0(\mathbb{Q})$. Pela proposição que acabamos de provar, existe n_0 tal que $a_n \neq 0$, para todo $n > n_0$. Então construa (a_n') tal que $a_n' = 1$, se $n < n_0$, e $a_n' = a_n$, para $n \geq n_0$. É claro que $\overline{(a_n)} = \overline{(a_n')}$ e, portanto, $a = \overline{(a_n)}$. Mas todo a_n' é diferente de zero e então $\overline{(b_n)} = \overline{(a_n')^{-1}}$ é o inverso de a, donde concluímos que $\mathbb{R}$ é um corpo. As proposições 2.11 e 3.11 implicam que, para cada $r \in \mathbb{Q}$, a sequência constante $(r, r, ..., r, ...)$ é um elemento do conjunto $S_c(\mathbb{Q})$.

Assim, para cada $r \in \mathbb{Q}$, podemos associar a classe de equivalência $\overline{(r)} \in \mathbb{R}$. Essa associação determina uma bijeção entre $\mathbb{Q}$ e um subconjunto $\mathbb{Q}'$ de $\mathbb{R}$. Identificamos r com $\overline{(r)}$ e passamos a considerar $\mathbb{Q}$ como um subconjunto de $\mathbb{R}$. Os elementos de $\mathbb{R}$ que não estão em $\mathbb{Q}'$ são chamados de *números irracionais*.

Para definir uma relação de ordem em $\mathbb{R}$, vejamos o seguinte corolário da proposição 5.11.

Corolário 1.11

Seja $(a_n) \in S_c(\mathbb{Q})$. Se $(a_n) \notin S_o(\mathbb{Q})$ e existe $n_o \in \mathbb{N}$ tal que para $n \geq n_o$, tem-se $a_n > 0$, então existem $\varepsilon \in \mathbb{Q}$, $\varepsilon > 0$, e $n \in \mathbb{N}$ tais que se $n \geq n_1$ então $a_n > \varepsilon$.

Demonstração

Pela proposição 5.11, existem $n_0' \in \mathbb{N}$ e $\varepsilon \in \mathbb{Q}$, $\varepsilon > 0$, tais que $|a_n| > \varepsilon$, se $n > n_0'$. Agora, faça $n_1 = max\ \{n_0', n_0\}$.

Dizemos que uma sequência (a_n) *possui a propriedade P* se (a_n) satisfaz as condições do corolário 1.11 e deixamos para o leitor a prova do seguinte lema.

Lema 1.11

Sejam (a_n) e (b_n) elemento de $S_c(\mathbb{Q})$. Se $(a_n) \approx (b_n)$ e (a_n) possui a propriedade P, então (b_n) também possui tal propriedade.

A relação de ordem em $\mathbb{R}$ é agora definida da seguinte forma: dados $a = (\underline{a_n})$, $b = (\underline{b_n}) \in \mathbb{R}$, dizemos que $a \leq b$ se $(b_n - a_n)$ possui a propriedade P ou se $(b_n - a_n) \in S_c(\mathbb{Q})$. Não é difícil verificar que essa relação é uma relação de ordem em $\mathbb{R}$.

Teorema 1.11

O corpo $\mathbb{R}$ é arquimediano.

Demonstração

Suponha $a = \overline{(a_n)}$, $b = \overline{(b_n)} \in \mathbb{R}$ e $0 < b < a$. Como (a_n) é de Cauchy, existe $M \in \mathbb{Q}$ tal que $a_n < M$, para todo $n \in \mathbb{N}$ e como $0 < b$, existem $\varepsilon \in \mathbb{Q}$, $\varepsilon > 0$ e $n_o \in \mathbb{N}$ tais que $b_n > \varepsilon$ se $n \geq n_0$. Como $\mathbb{Q}$ é arquimediano (ver exercício 10.4, para reforçar), existe $m \in \mathbb{N}$ tal que $M < m.\varepsilon$ ou seja $c = \overline{(m)}$ é tal que $c.b = \overline{(c.b_n)} > a$, pois $c\ .\ b_n - a_n > M - a_n > 0$, para todo $n \geq n_o$.

Finalmente, veremos que as sequências de Cauchy em $\mathbb{R}$ são convergentes. Adotaremos as mesmas definições usados em $\mathbb{Q}$ para sequências convergentes e sequências de Cauchy em $\mathbb{R}$. Naturalmente, há necessidade de adaptar a notação. Por exemplo, onde lá tínhamos $\varepsilon \in \mathbb{Q}$, $\varepsilon > 0$ aqui escrevemos simplesmente $\varepsilon > 0$. No resto, as definições são as mesmas.

Lema 2.11

Para cada $a \in \mathbb{R}$, existe uma sequência $(a_n) \in S(\mathbb{Q})$ que converge para a em $\mathbb{R}$

Demonstração

Suponha, sem perda de generalidade, que $a > 0$. Como $\mathbb{R}$ é arquimediano, o conjunto $B_n = \{j \in N \mid \frac{j}{2^n} > a\}$ é não vazio. Assim definimos j_n como sendo o elemento mínimo de B_n, $n \in \mathbb{N}$. Logo $\frac{1}{2^n}(j_n - 1) < b \leq \frac{1}{2^n} j_n$, ou $0 \leq \frac{j_n}{2^n} - b < \frac{1}{2^n}$ e teremos então $0 < \frac{1}{2^n}.j_n - b \leq \frac{1}{2^n}$ (1)

Ora, da demonstração do teorema 1.11, podemos deduzir que na definição de limite em $\mathbb{R}$, basta considerar $\varepsilon \in \mathbb{Q}$, $\varepsilon > 0$ e assim de (1) resulta que a sequência $\left(\frac{j_n}{2^n}\right) \in S(\mathbb{Q})$, converge para a em $\mathbb{R}$.

Lema 3.11

Suponha que (a_n) é de Cauchy em $\mathbb{Q}$. Então $\overline{(a_n)}$ converge em $\mathbb{R}$.

Demonstração

Considere $a = \overline{(a_n)} \in \mathbb{R}$. Vamos mostrar que $lim\ \overline{(a_n)} = a$. Cada a_n é naturalmente identificado com a classe da sequência constante, $a_n = (a_n, a_n, \ldots, a_n, \ldots)$. Então

$$\overline{a - a_1} = \overline{(0, a_2 - a_1,\ a_3 - a_1, \ldots,\ a_n - a_1, \ldots)},$$

$$\overline{a - a_2} = \overline{(a_1 - a_2, 0,\ a_3 - a_2, \ldots,\ a_n - a_2, \ldots)},$$

. . .

$$\overline{a - a_m} = \overline{(a_1 - a_m,\ a_2 - a_m, \ldots,\ a_n - a_m, \ldots)},$$

Como (a_n) é de Cauchy, dado $\varepsilon \in \mathbb{Q}$, $\varepsilon > 0$, existe $n_0 \in \mathbb{N}$ tal que se $n, m \geq n_0$, então $|a_n - a_m| < \varepsilon$, ou seja, $lim\ a_n = a$.

Chegamos ao principal resultado deste capítulo.

Teorema 2.11

Em $\mathbb{R}$, toda sequência de Cauchy é convergente.

Demonstração

Seja (a_n) uma sequência de Cauchy em $\mathbb{R}$. Pelo lema 3.11, para cada $n \in \mathbb{N}$, existe uma sequência de racionais $(a_{in})_i \in \mathbb{N}$ que converge em $\mathbb{R}$ para a_n. Seja $\varepsilon \in \mathbb{Q}$, $\varepsilon > 0$. Então, para cada $n \in \mathbb{N}$ escolha um a_{in} tal que $|a_{in} - a_n| < \varepsilon$ e faça $b_n = a_{in}$. Como (a_n) é de Cauchy, existe

$n_0 \in \mathbb{N}$ tal que, se $n, m \geq n_0$, $|a_m - a_n| < \varepsilon$. Assim para tais m, n temos $|b_n - b_m| \leq |b_n - a_n| + |a_n - a_m| + |b_m - a_m| < 3\varepsilon$, o que mostra que (b_n) também é de Cauchy. Pelo lema 3.11, (b_n) converge para $\overline{(b_n)} = b$. Isso garante que existe $n_0 \in \mathbb{N}$ tal que $|b_n - b| < \varepsilon$, se $n \geq n_0$. Finalmente, $|a_n - b| \leq |a_n - b_n| + |b_n - b| < 2\varepsilon$, para todo $n \geq n_0$, o que prova que $lim\ a_n = b$.

Bibliografia

AGRAWAL, M., KAYAL, N. e SAXENA, N. *Primes is in P".* Annals of Mathematics. **160** (2), 781–793, USA, 2004.

ALBERTSON, M. O. e HUTCHINSON, J. P., *Discrete Mathematic with Algoritms*. John Wiley & Sons, Inc., USA, 1998.

BIRKHOFF, G e MACLANE S., *Álgebra moderna básica*. Guanabara Dois, Rio de Janeiro, 1980.

CASTRUCCI, B., *Fundamentos da geometria: estudo axiomático do plano euclidiano*. Livros Técnicos e Científicos, Rio de Janeiro, 1978.

COUTINHO, S. C., *Números Inteiros e Criptografia RSA*. IMPA/SBM (Série de Computação e Matemática), Rio de Janeiro, 1997.

COUTINHO, S. C., *Primalidade em Tempo Polinomial*. SBM (Coleção Iniciação Científica), Rio de Janeiro, 2004.

EVARISTO, J., *Programando com Pascal*. Terceira Edição. Edição digital (www.ic.ufal.br/professor/jaime), Maceió, 2008.

FIGUEIREDO, D. G., *Análise I*. Livros Técnicos e Científicos. Editora, Rio de Janeiro, 1975.

GONÇALVES, A., *Introdução à Álgebra*. IMPA (Projeto Euclides), Rio de Janeiro, 1979.

HEFEZ, A., *Curso de Álgebra*, Volume 1. Instituto de Matemática Pura e Aplicada (Coleção Matemática Universitária), Rio de Janeiro,

1993.

JACY MONTEIRO, L. H., *Elementos de Álgebra*. Ao Livro Técnico e Científico S. A., Rio de Janeiro, 1969.

KNUTH, D. E., *The Art of Computer Programming*, volume 2, *Seminumerical Algorithms*. Addison-Wesley Publishing Company, USA, 1988.

LEMOS, M., *Criptografa, números primos e algoritmos*. IMPA (17º Colóquio Brasileiro de Matemática), Rio de Janeiro, 1989.

LIMA, E. L. e outros, *A Matemática do Ensino Médio*, volume 1. Sociedade Brasileira de Matemática (Coleção do Professor de Matemática), Rio de Janeiro, 1996.

LIMA, E. L., *Análise Real*, volume 1. IMPA (Coleção Matemática Universitária), Rio de Janeiro, 1993.

RIVEST, R. L., SHAMIR A. e ADLEMAN, L., *A method for obtaining digital signatures and public-key cryptosystems*, Comm. ACM, 21, 120-126.

SINGH, S., *O Último Teorema de Fermat: a história do enigma que confundiu as maiores mentes do mundo durante 358 anos*. Record, Rio de Janeiro, 1998.

WILES, A., *Modular eliptic curves and Fermat's Last Theorem*. Annals of Mathematics 142, 443-551, USA, 1995.

Índice Remissivo

E

F

G

H

I

J

L

M

N

O

P

Q

R

S

T

U

V

Z