Jaime Evaristo
Eduardo Perdigão

INTRODUÇÃO À ÁLGEBRA ABSTRATA

(Com aplicações à Ciência da Computação e o estudo do Sistema de Criptografia RSA)

EuclidesDiofanteFermatEratóstenesEulerMersenne
PitágorasWilsonBernoulliNewtonCauchy

$(f \circ g)(x) = f(g(x))$; se $p|(a.b)$, então $p|a$ ou $p|b$; $\emptyset \subset A$

$a = b \cdot q + r$; $6 \cdot 4 = 0$; $a + (b + c) = (a + b) + c$;

$a = c_n.b^n + c_{n-1}.b^{n-1} + \ldots + c_2.b^2 + c_1.b + c_0$; $a \equiv b \bmod n$

Segunda Edição/Formato Digital/Versão 01.2013
Instituto de Computação – Universidade Federal de Alagoas

Jaime Evaristo
Mestre em Matemática
Professor Adjunto
Instituto de Computação
Universidade Federal de Alagoas

Eduardo Perdigão
Doutor em Matemática
Professor Aposentado
Instituto de Matemática
Universidade Federal de Alagoas

Introdução à Álgebra Abstrata

Segunda Edição
Formato Digital/Versão 01.2013
Maceió, junho de 2013

Sumário

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 dela 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 este motivo e por excelência, a linguagem da Ciência. Além disto, o ato de estudar Matemática desenvolve o raciocínio do estudante e isto permite que ele seja capaz de compreender com mais facilidade os conceitos de outros ramos do conhecimento humano e as inter-relações entre estes 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 disto, 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, num 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 121 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 (as soluções de todas as questões estão disponíveis em www.ccen.ufal.br/jaime). 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@ccen.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 citada editora pelo empenho em publicar esta obra.

Maceió, julho de 2002
Jaime Evaristo
Eduardo Perdigão

Prefácio (da atual edição)

Esta segunda edição é uma revisão bastante 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, dentre outras modificações.

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 bastante efetiva dos alunos Gerlivaldo Felinto da Silva e Leonildo de Mello Nascimento. Também gostaríamos de agradecer as participação 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; em 2014, Victor Gabriel Lima, Daniel Tenório e Manoela Cássia dos Santos também contrubuíram na caminhada para o "erro zero".

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 estas participações. Toda e qualquer observação deve ser encaminhada para jaime@ccen.ufal.br, com o assunto LIVRO INTRODUÇÃO À ÁLGEBRA ABSTRATA.

Maceió, dezembro de 2013
Jaime Evaristo
Eduardo Perdigão

1. Conjuntos e Funções

1.1 Entes primitivos

Segundo o Dicionário Aurélio, *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. Exemplos claros de "definições" que pecam em relação ao segundo aspecto levantado são: um *ponto* é a interseção de duas *retas* e uma *reta* é um conjunto de *pontos alinhados*. Com estas "definições", para se entender o que é um *ponto* seria necessário saber o que é uma *reta* e para compreender o que é uma *reta* é indispensável se saber o que é um *ponto* e o que são *pontos alinhados*.

Em alguns livros de Matemática do ensino médio encontra-se a seguinte "definição" de conjunto: *conjunto é uma coleção de objetos*. O problema agora é que esta "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.

Algumas ciências, como a Matemática e a Física, necessitam considerar entes, relações ou grandezas que não são definidos, ditas então *entes primitivos*, *grandezas primitivas* ou relações estabelecidas *primitivamente*. Por exemplo, *ponto*, *reta* e *plano* são *entes primitivos* da Geometria Euclidiana enquanto que o *tempo*, a *distância* e a *massa* são *grandezas primitivas* da Mecânica Newtoniana.

Estabelecidos os entes primitivos de uma ciência, pode-se então se definir novos objetos, e a partir destes, definir-se novos outros objetos, e assim por diante. Por exemplo, a partir das grandezas físicas da Mecânica pode-se definir *velocidade* como o quociente entre a *distância* percorrida e o *tempo* gasto para percorrê-la implicando no fato de que *velocidade* não é uma grandeza primitiva. A partir da grandeza física não primitiva *velocidade* e da grandeza primitiva *tempo* pode-se definir *aceleração* como sendo a variação da velocidade na unidade de tempo.

1.2 Conjuntos

Em Matemática, *conjunto* é um *ente primitivo* e portanto não é definido. Entendemos *conjunto* como uma coleção de objetos, no sentido coloquial do termo. Os objetos que compõem a coleção que está sendo considerada um conjunto são chamados *elementos* do referido conjunto.

De um modo geral, conjuntos são representados por letras maiúsculas e seus elementos por letras minúsculas. Se A designa um conjunto e a é um dos elementos, dizemos que *a pertence a A*, isto sendo simbolizado por $a \in A$. Estabelecemos então, também de forma *primitiva*, a relação de *pertinência* entre um conjunto e seus elementos. 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 podemos apresentar um exemplo de um objeto da Matemática que é definido a partir dos entes primitivos *ponto*, *reta*, *plano* e *conjunto* e da grandeza primitiva *distância*: dados um plano α, um ponto p pertencente a α e um número real r, a *circunferência* de *centro p*, de *raio r* e contida no plano α é o conjunto dos pontos do plano α situados a uma distância r do ponto p.

1.3 Igualdade

Na linguagem coloquial, dois objetos são ditos *iguais* quando são do mesmo tipo e têm a

mesma aparência. Não tem sentido se dizer que uma cadeira é igual a um sofá; se é dito que duas cadeiras são iguais elas são praticamente indistinguíveis a uma simples espiada.

Em Matemática, o conceito de *igualdade* é considerado primitivo, entendendo-se 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 $\neq$.

Vamos admitir primitivamente que as seguintes afirmações são verdadeiras:

1. Todo objeto é igual a ele mesmo: $a = a$, qualquer que seja o objeto a.
2. Se um objeto é igual a outro, este é igual àquele: se $a = b$, então $b = a$;
3. Dois objetos iguais a um terceiro objeto são iguais entre si: se $a = b$ e $b = c$, então $a = c$.

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. Isto será feito na seção 1.7.

1.4 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. Neste caso, também podemos escrever $B \supset A$, que é lido *B contém A*. A negação de $A \subset B$ é indicada por $A \not\subset B$ e, evidentemente, 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 $A \subset C$.

Qualquer argumento que justifica a veracidade de uma assertiva matemática é chamado *demonstração* ou *prova* daquela afirmação.

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.

1.5 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 que se está utilizando. 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

$$B = \{\{a\}, \{a, b\}, \{a, b, c\}, ...,\{a, b, c, ...,z\}\}.$$

Observe que os elementos do conjunto B são subconjuntos do conjunto das letras do alfabeto.

1.6 As expressões "se, então" e "se e somente se"

Os dicionários da língua portuguesa apresentam, entre outras acepções, o vocábulo *então* na classe gramatical advérbio significando: *nesse caso*, *assim sendo*, *em tal caso*. Nesse sentido, o *então* sempre (ou quase sempre, por precaução) é precedido de uma oração que se inicia pela conjunção *se*, a qual define o "nesse caso", o "assim sendo", o "em tal caso": "amanhã, *se* fizer sol, *então* iremos à praia"; "*se* você não estudar, *então* você não será aprovado".

Observe que a afirmação "amanhã, *se* fizer sol, *então* iremos à praia" não será desdita se no dia seguinte não fizer sol e, mesmo assim, o grupo tiver ido à praia. A afirmação fez referência ao programa que seria feito na hipótese de "fazer sol". Nada foi dito em relação ao que seria feito se "não fizesse sol".

Se p e q são duas afirmações matemáticas, a assertiva *se p, então q* estabelece que a veracidade de p implica a veracidade de q: se p ocorrer, q também ocorre. Para a ocorrência de q é *suficiente* que p ocorra.

Se a afirmação anterior fosse "amanhã, se fizer sol, e só nesta hipótese, iremos à praia", a situação seria outra. Neste caso, se no dia seguinte fizer sol, o grupo vai à praia. Se no dia seguinte o grupo foi à praia é porque fez sol. A Matemática ao invés de usar o "e só nesta hipótese" utiliza a expressão "se e somente se" e altera a ordem das afirmativas: "amanhã iremos à praia se e somente se fizer sol".

Se p e q são duas afirmações matemáticas a assertiva *p se e somente se q* estabelece que a veracidade de p implica a veracidade de q e, reciprocamente, a veracidade de q acarreta a veracidade de p: se p ocorrer, q também ocorre (a ocorrência de p é *suficiente* para a ocorrência q); se q ocorrer, p também ocorre ou se q ocorreu, p também ocorreu (a veracidade de p é *necessária* para a veracidade de q).

Uma afirmação do tipo "se p, então q" pode ser enunciada "*p implica q*" ou "p é *condição suficiente* para q" ou, ainda, "*q é condição necessária para p*".

Uma afirmação do tipo "p se e somente se q" pode ser enunciada "p e q são *equivalentes*" ou, combinando o estabelecido no parágrafo anterior, "p é *condição necessária e suficiente* para q". Voltaremos a falar sobre isso na seção 1.13.

Observe que a expressão "se, então" já foi utilizada no estabelecimento das afirmações que estabelecemos que são verdadeiras para a igualdade de objetos matemáticos.

1.7 Igualdade de conjuntos

Como foi dito anteriormente, a igualdade de objetos matemáticos é um conceito primitivo significando que quando dois objetos são iguais eles podem ser considerados o mesmo objeto.

A igualdade entre dois conjuntos é estabelecida da seguinte forma: dois conjuntos A e B 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.

Observe que para dois conjuntos A e B *possuírem* os mesmos elementos *(e, portanto, serem iguais*) é suficiente que todo elemento de A seja elemento de B e que todo elemento de B seja elemento de A. Ou seja, para dois conjuntos A e B *possuírem* os mesmos elementos *(e, portanto,*

serem iguais) é suficiente que A seja subconjunto de B e que B seja subconjunto de A.

Assim podemos definir igualdade de conjuntos A e B por: $A = B$ se e somente se $A \subset B$ e $B \subset A$.

Esta 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. Assim os conjuntos $A = \{a, b, c\}$ e $B = \{b, c, a\}$ 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.

1.8 Par ordenado e produto cartesiano

Teremos necessidade de trabalhar com pares de elementos de dois conjuntos dados, considerados numa 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 $\{\{a\}, \{a, b\}\}$. Naturalmente, os conjuntos A e B podem ser iguais, definindo-se então par ordenado de dois elementos de um mesmo conjunto. Nesse caso, podemos ter par do tipo (a, a). Evidentemente, $(a, a) = \{\{a\}\}$.

Sobre pares ordenados é verdadeira a seguinte afirmação.

Sejam A e B dois conjuntos e $a, a' \in A$ e $b, b' \in B$. Temos que $(a, b) = (a', b')$ se e somente se $a = a'$ e $b = b'$.

De fato, se $a = a'$ e $b = b'$ temos $\{a\} = \{a'\}$ e $\{a, b\} = \{a', b'\}$ o que implica $\{\{a\}, \{a, b\}\} = \{\{a'\}, \{a', b'\}\}$.

Suponhamos agora que $(a, b) = (a', b')$. Se $a = b$, temos que os conjuntos $A = \{\{a\}\}$e $A' = \{\{a'\}, \{a', b'\}\}$ são iguais o que só acontece se $a' = b' = a$. Se $a \neq b$, temos $\{a'\} \neq \{a, b\}$ e a igualdade dos conjuntos $A = \{\{a\}, \{a, b\}\}$ e $A' = \{\{a'\}, \{a', b'\}\}$ implica $\{a\} = \{a'\}$ e $\{a, b\} = \{a', b'\}$ o que acarreta $a = a'$ e $b = b'$.

A veracidade desta afirmação, além de justificar a denominação *par ordenado*, permite que se distinga os elementos que compõem o par (a, b): a é a *primeira componente* e b é a *segunda componente*.

Uma afirmação verdadeira sobre um ente matemático é chamada de *propriedade* daquele ente. Assim, a afirmação "$(a, b) = (a', b')$ se e somente se $a = a'$ e $b = b'$" é uma *propriedade* dos pares ordenados.

O *produto cartesiano* de dois conjuntos A e B, indicado por $A \times B$, é o conjunto dos pares ordenados com primeiras componentes no conjunto A e segundas componentes no conjunto B. Por exemplo, se $A = \{a, c, d\}$ e $B = \{e, f\}$, o produto cartesiano de A por B é o conjunto $A \times B = \{(a, e), (a, f), (c, e), (c, f), (d, e), (d, f)\}$ e o produto cartesiano de B por A é o conjunto $B \times A = \{(e, a), (e, c), (e, d), (f, a), (f, c), (f, d)\}$, exemplo que já mostra que, de um modo geral, $A \times B \neq B \times A$.

É comum se utilizar a notação A^2 para representar o produto cartesiano $A \times A$. Assim, no exemplo acima temos $B^2 = \{(e, e), (e, f), (f, f), (f, e)\}$ e $A^2 = \{(a, a), (a, c), (a, d), (c, a), (c, c), (c, d), (d, a), (d, c), (d, d)\}$.

1.9 Relações binárias

Em muitas situações, é necessário e útil relacionar (no sentido usual do termo) elementos de um ou de dois conjuntos. Esta relação pode ser estabelecida através dos pares ordenados que se pretende relacionar. Se A e B são dois conjuntos, qualquer subconjunto do produto cartesiano $A \times B$ é chamado de uma *relação binária entre A e 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*.

Por exemplo, se A é o conjunto das vogais e B é o conjunto das consoantes os conjuntos $R = \{(a, b), (e, f), (i, j), (o, p), (u, v)\}$, $S = \{(a, x), (e, g), (i, b)\}$ e $T = \{(e, m), (i, z)\}$ são relações binárias entre A e B (ou de A *em* B).

Normalmente, 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* 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 R satisfaz a esta condição pois cada segunda componente é a consoante que sucede a vogal primeira componente. As componentes dos pares das outras relações dos exemplos não guardam nenhuma relação entre si e, portanto, não são relevantes.

Utilizando uma barra vertical significando *tal que*, pode-se representar uma relação entre dois conjuntos por $R = \{(x, y) \in A\text{x}B| \ ...\}$, onde em … é colocada a *regra* que estabelece a relação entre x e y. Muitas vezes, associa-se um símbolo a uma relação definida num conjunto A. Neste caso, se o símbolo da relação é #, a indicação de que um par (a, b) pertence à relação é feita por $a \# b$.

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 que y está sendo utilizado para representar todos os elementos do conjunto B. Neste caso dizemos que os símbolos x e y são *indeterminadas* ou *variáveis* dos conjuntos referidos.

Uma relação definida num conjunto A pode ser adjetivada de acordo com algumas propriedades que ela satisfizer. Dizemos que uma relação R num conjunto A é:

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

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

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

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

•*total* se quaisquer que sejam $x, y \in A$, $(x, y) \in R$ e/ou $(y, x) \in R$, onde o "e/ou" indica que podem ocorrer as duas pertinências ou apenas uma delas.

As definições anteriores estabelecem quando o adjetivo respectivo pode ser aplicado a uma relação binária. Como fizemos com a definição de subconjunto, é interessante observar as condições mínimas que negam as definições anteriores e, portanto, tal adjetivo não pode ser associado à relação. Com o desenvolvimento de um raciocínio simples, temos que uma relação R num conjunto A

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

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

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

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

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

Por exemplo, se A 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 A é o conjunto das vogais e consideremos a relação $\{(x, y) \in A\text{x}A|\text{y} = \text{x}\}$. Como cada vogal só é igual a ela mesma, os pares desta 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*.

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 $\wp(A)$. Como os elementos de $\wp(A)$ são conjuntos cujos elementos são elementos do conjunto A, podemos definir a relação (chamada *inclusão*) $\mathrm{I} = \{(X, Y) \in \wp(A)\mathrm{x}\wp(A) \mid X \subset Y\}$. As propriedades apresentadas na seção 1.4 mostram que esta relação é reflexiva e transitiva. A definição de igualdade de conjuntos garante que a inclusão é antissimétrica.

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

1.10 Funções

Estamos agora interessados em relações entre dois conjuntos A e B em que cada elemento de A esteja relacionado com um único elemento de B. Uma relação que satisfaz a esta propriedade é chamada *função*, definida formalmente como segue.

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 é necessário e suficiente que para todo $x \in A$ exista $y \in B$ tal que $(x, y) \in f$ e que se $(x, y_1) \in f$ e $(x, y_2) \in f$ então $y_1 = y_2$.

Por exemplo, se A é o conjunto das vogais e B é o conjunto das consoantes, a relação entre A e B dada por $f = \{(a, b), (e, f), (i, j), (o, p), (u, v)\}$ é uma função de A em B. Por outro lado, se $A = \{a, b, c\}$, a relação $I = \{(X, Y) \in \wp(A)\mathrm{x}\wp(A) \mid X \subset Y\}$ não é uma função de $\wp(A)$ em $\wp(A)$ pois $(\{a\}, \{a, b\}) \in I$ e $(\{a\}, \{a, c\}) \in I$ e como $\{a, b\} \neq \{a, c\}$, o elemento $X = \{a\}$ estaria relacionado com $Y_1 = \{a, b\}$ e $Y_2 = \{a, c\}$.

Como já vimos fazendo, utilizaremos letras minúsculas f, g, h, etc., para representar funções e escreveremos $y = f(x)$, para indicar que $(x, y) \in f$. Neste caso diremos que y é a *imagem* do *objeto* x pela função f. No futuro, usaremos também cadeia de caracteres para indicar funções.

Se f é uma função de um conjunto A em um conjunto B, o conjunto A é chamado *domínio* 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 $f(A)$.

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

$$\begin{aligned} f : A &\to B \\ x &\to f(x). \end{aligned}$$

Nesse caso, $y = f(x)$ 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 os diversos valores dos objetos. Por exemplo, se A é o alfabeto podemos definir a função g de A em A por $g(x) = a$, se $x = z$ e $g(x)$ é a letra sucessora de x se $x \neq z$. Num caso como este, pode-se utilizar expressões como *caso contrário*, *senão*, *em outra hipótese* para indicar as situações em que a última *sub-regra* será aplicada. Isto será utilizado na seção 1.13.

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 e suficiente que para todos os elementos k e j do domínio de f 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 destes 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* função.

Dois exemplos de funções que serão utilizadas em exemplos e demonstrações futuras são apresentadas 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 conjunto das letras do alfabeto, g é a função de A em A que associa a cada letra a letra que a sucede no alfabeto (considerando a como a letra sucessora de z) e V é o conjunto das vogais, a função g restrita ao conjunto V é a função $g_{/V} = \{(a, b), (e, f), (i, j), (o, p), (u, v)\}$.

1.11 O Conjunto Vazio

Vimos acima que um conjunto pode ser representado pela exibição de seus elementos entre chaves. 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 {V, F} (V significando *verdadeiro* e F, *falso*) é chamado *conjunto de Boole*. Um *predicado* ou uma *sentença aberta* num conjunto A é uma função de A no conjunto de Boole.

Como as imagens dos objetos podem ser apenas V ou F, um predicado pode ser definido estabelecendo-se quando a imagem de um objeto será V e quando ela será F.

Por exemplo, se A é o conjunto das letras do alfabeto, pode-se definir um predicado em A por $p(x) = \text{V}$ se e somente se x é uma vogal. Neste caso, temos, por exemplo, $p(a) = \text{V}$ e $p(b) = \text{F}$. 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. Para a letra x, temos $p(x) = \text{F}$. 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. Esta observação permite que um predicado seja definido explicitando apenas a tal propriedade a qual ele se refere. Assim, o predicado *p(x) = V se e somente se x é uma vogal* pode ser referido apenas por *x é uma vogal*. Vamos estabelecer também que uma definição de um predicado prescinde da expressão *se e somente se*. O predicado *p(x) = V se e somente se x é uma vogal* pode ser definido apenas por *p(x) = V se 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 $p(x) = \text{V}$. Por exemplo, se A é o conjunto das letras do alfabeto, o conjunto das vogais pode ser representado por $B = \{x \in A | \ x \text{ é uma vogal}\}$.

Um predicado p num conjunto A é uma *contradição* se $p(x) = \text{F}$ para todo elemento $x \in A$ e é uma *tautologia* se $p(x) = \text{V}$ 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 e é chamado *conjunto vazio*, sendo simbolizado por $\varnothing$. Por exemplo, se A é um conjunto qualquer o conjunto $\{x \in A|\ x \neq x\}$ é o conjunto vazio. Um conjunto diferente do conjunto vazio é dito *não vazio*.

Na seção 1.14 provaremos que o conjunto vazio é subconjunto de qualquer conjunto: $\varnothing \subset A$, qualquer que seja o conjunto A.

1.12 Operações

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.

Por definição, uma *operação* num conjunto A é uma função do produto cartesiano AxA no próprio conjunto A. Por exemplo, no conjunto das vogais podemos definir a operação f dada pela tabela a seguir, na qual o elemento da linha i e da coluna j fornece 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

Os autores, humildemente, concordam com o leitor que este exemplo não é muito esclarecedor. Nas seções seguintes teremos exemplos mais consistentes de operação. Nestes 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.

Naturalmente, podem ser realizadas aplicações sucessivas de uma operação. Neste caso, usa-se parênteses para indicar quais resultados "parciais" devem ser obtidos. Utilizando o operador + para a operação do exemplo anterior e chamando o resultado da operação de *soma*, $(a + e) + o$ indica que deve-se 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*.

Como as relações binárias, as operações também podem ser adjetivadas de acordo com propriedades que ela satisfizer. Seja A um conjunto e # uma operação em A. Dizemos que a operação #

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

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

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

Quando a operação está denotada na forma de função $f(a, b)$, forma de representação chamada *notação prefixa*, as classificações acima são assim referenciadas:

Uma operação f definida num conjunto A

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

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

•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 $e' \# e'' = e'' \# e' = e'$, pois e'' é *elemento neutro* e $e'' \# e' = e' \# e'' = e''$, pois e' é elemento neutro, implicando então, pela transitividade da igualdade, $e' = e''$. Portanto se encontrarmos um elemento neutro de uma operação ele é **o** elemento neutro desta operação.

A operação no conjunto das vogais definida acima é comutativa e possui elemento neutro, u. Embora seja bastante enfadonho (teria que se verificar que $x + (y + z) = (x + y) + z$ para todos os casos) é fácil mostrar que a operação também é associativa. Por exemplo, $a + (e + o) = a + a = e$ que, como já foi visto, é igual a $(a + e) + o$.

Numa operação associativa, não há a necessidade da colocação de parênteses. Se # é o operador de uma operação associativa, como $a \# (b \# c) = (a \# b) \# c$, podemos indicar $a \# (b \# c)$ por $a \# b \# c$, como se estivesse operando três operandos. Esta 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 acima temos, por exemplo,

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

Além da comutatividade, associatividade e existência de elemento neutro, uma operação pode ser adjetivada 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 $a, b, c \in A$. Esta propriedade é referida como *distributividade* de # em relação à *.

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 destas propriedades.

1.13 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*) permitem o estabelecimento de uma linguagem que facilita sobremaneira o discurso matemático.

Dado um conjunto não vazio A, representemos por $Pred(A)$ o conjunto dos predicados em A. Ou seja, $Pred(A)$ é o conjunto de todas as funções de A no conjunto de Boole {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 $p, q \in Pred(A)$.

•*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 linguagem coloquial: se o/a chefe da família 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 $p(x) = q(x) = \text{V}$ então $q(x) = p(x) = \text{V}$), a conjunção é comutativa. Ela também é associativa: se p, q e r são predicados em

A, por um lado $((p \wedge q) \wedge r)(x) = \mathrm{V}$ se $(p \wedge q)(x) = r(x) = \mathrm{V}$ o que só acontece se $p(x) = q(x) = r(x) = \mathrm{V}$ e por outro lado $(p \wedge (q \wedge r))(x) = \mathrm{V}$ se $p(x) = (q \wedge r)(x) = \mathrm{V}$ o que só acontece também se $p(x) = q(x) = r(x) = \mathrm{V}$. Claramente, uma tautologia τ é o elemento neutro da conjunção.

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

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

Isto é, a *disjunção* de dois predicados p e q é verdadeira se e somente se um dos predicados for verdadeiro ou se ambos forem verdadeiros. Observe agora que a denominação **ou** para o operador $\vee$ não corresponde exatamente ao uso da conjunção **ou** na linguagem comum: se o/a chefe da família 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 que o **ou** da linguagem coloquial é *exclusivo*. Embora os dicionários não apresentem esta possibilidade, é relativamente comum se usar **e/ou** na linguagem coloquial quando se pretende se expressar um "ou inclusivo". Às vezes, a Matemática ao utilizar um vocábulo modifica (quase sempre, ligeiramente) o seu significado. Surge então a *linguagem matemática*, muito útil para o mundo científico. 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 claramente 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.

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

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

O predicado $p \Rightarrow q$ também pode ser lido *se p, então q* e quando p e q são verdadeiros tem a conotação dada na seção 1.6. Observe que $p \Rightarrow q$ só é falso se p é verdadeiro e q é falso. Assim, ao contrário da linguagem comum, na qual *implicar* é utilizado numa relação de causa e efeito, em 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 da adolescente, a dois meses do certame, adquire um automóvel e anuncia para ela: *se você for aprovada, então 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. Normalmente, 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).

•*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 tem a mesma conotação dada à expressão *se e somente se* discutida na seção 1.6. É fácil ver que uma *equivalência* pode ser obtida a partir de uma *conjunção* de *implicações*, reiterando o que foi dito na referida seção. Na verdade temos a seguinte igualdade: $p \Leftrightarrow q = (p \Rightarrow q) \wedge (q \Rightarrow p)$.

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 {V, F}) e para cada x de A se tenha $r(\text{x}) = s(\text{x})$. Basta então mostrar a igualdade $r(\text{x}) = s(\text{x})$, 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 $r(\text{x})$ e $s(\text{x})$. 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.

1.14 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 isto, consideremos a seguinte definição. A *negação* de um predicado p é o predicado indicado por $\sim p$ tal que $(\sim p)(x) = \text{F}$ se $p(x) = \text{V}$.

Como é fácil provar que (ver exercício 1.9) se p e q são predicados num conjunto A, tem-se $(p \Rightarrow q) = ((\sim q) \Rightarrow (\sim p))$, uma 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.

Por exemplo, para demonstrar que o conjunto vazio é subconjunto de qualquer conjunto (ver seção 1.11), suponhamos que exista um conjunto A tal que $\varnothing \not\subset A$ (negação da tese). Daí teríamos que existe 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 1.10) que $(p \Rightarrow q) = ((p \wedge (\sim q)) \Rightarrow \gamma)$, onde p e q são predicados num 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.

1.15 Operações com conjuntos

Seja U um conjunto e consideremos $\wp(U)$ o conjunto das partes de U. Normalmente, quando

se está trabalhando com conjuntos que são subconjuntos de um conjunto U, este conjunto U é chamado *conjunto universo*.

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 $A, B \subset U$:

•*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.

•*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.

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

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

Aplicando novamente a definição de *conjunção*, observa-se que a *diferença* entre dois conjuntos A e B é o conjunto dos elementos que pertencem exclusivamente ao conjunto A.

Para um exemplo, sejam U o conjunto das letras do alfabeto, $A = \{a, c, e, f\}$ e B {c, d , *f*, g}. Temos $A \cup B = \{a, c, d, e, f, g\}$, $A \cap B = \{c, f\}$, $A - B = \{a, e\}$ 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 que mostra que um ente matemático não goza de uma determinada propriedade é chamado de *contraexemplo*). É fácil se 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 mesmo sendo verdade que $A - \varnothing = A$, o conjunto vazio não é elemento neutro da diferença, pois, se $A \neq \varnothing$, $\varnothing - A \neq A$. Devido ao fato de que $A \cap U = A$, qualquer que seja o subconjunto de U, temos que o universo U é o elemento neutro da interseção.

1.16 Uma operação com funções

Seja A 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

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

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 $I_A \circ f = f \circ I_A = f$. Isto prova que a função identidade é o elemento neutro da composição de funções.

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

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

e

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

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 $(f \circ g)(x) = f(g(x))$.

Observe que esta definição não atende plenamente o conceito de operação num conjunto dada na seção 1.9, 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.

1.17 Funções inversíveis

Seja # uma operação num 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 $x \# y = y \# x = e$.

Suponhamos que a operação # seja associativa e que y' e y'' sejam simétricos de x. Temos

$y' = y' \#$ 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)

Assim, se um elemento x tem simétrico em relação a uma operação associativa, este simétrico é único. Para algumas operações, o simétrico do elemento x continua sendo chamado *simétrico de x* e é representado por -x. Para 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 $f \circ g = g \circ f = I_A$. Como a composição de funções é associativa, quando esta função g existe ela é única e chamada *inversa* da função f, sendo representada por f^{-1}. Nesse caso, dizemos que f é *inversível*.

Por exemplo, se A é o conjunto das vogais, a função $f \in \mathfrak{I}(A)$, $f = \{(a, e), (e, i), (i, o), (o, u), (u, a)\}$ 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 $f \circ f^{-1} = I_A$. Como também (o que é muito fácil verificar) $f^{-1} \circ f = I_A$, temos que f é inversível.

Por seu turno, a função g de $\mathfrak{I}(A)$, $g = \{(a, u), (e, u), (i, u), (o, u), (u, u)\}$ 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 $g \circ f = I_A$. Neste caso, e como acima, diz-se que g é a *função inversa* de A e indica-se g por f^{-1}.

Por exemplo, se A 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 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 *injetiva* (ou *injetora* ou uma *injeção*) se $x_1 \neq x_2$ implicar $f(x_1) \neq f(x_2)$. Em outros termos, numa função injetiva objetos diferentes têm sempre imagens diferentes. Ou ainda, numa *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 A 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.

Uma função $f \in \mathfrak{I}(A, B)$ é dita *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 que a função g não o é, pois $c \notin g(A)$.

Uma função $f \in \mathfrak{I}(A, B)$ é dita *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 $f \in \mathfrak{I}(A, B)$ 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 $f \circ g = I_B$, e $(g \circ f)(x) = g(f(x)) = g(y) = x$, 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 num 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 conjunto estabelece uma *correspondência biunívoca* ou uma *correspondência um a um* entre os dois conjuntos.

1.18 Exercícios

1.1. Verifique se cada uma das relações abaixo, definidas no conjunto de habitantes da terra (com os significados usuais da linguagem coloquial), 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 linguagem coloquial), 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 num 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 num 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 num 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 num conjunto A. Mostre que $(p \Rightarrow q) = (\sim p) \vee q$.

1.9. Sejam p e q predicados num conjunto A. Mostre que $(p \Rightarrow q) = ((\sim q) \Rightarrow (\sim p))$.

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

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

a) $(A \cup B) \cup C = A \cup (B \cup C)$ (isto é, a união de conjuntos é associativa)

b) $A \cap B \subset A$

c) $(A \cap B) \cap C = A \cap (B \cap C)$ (isto é, a interseção de conjuntos é associativa)

d) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ (isto é, a interseção de conjuntos é distributiva em relação à união)

e) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ (isto é, a união de conjuntos é distributiva em relação à interseção)

1.12. 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 $B = C$

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

1.14. Quando $A \subset B$ a diferença $B - A$ é chamada *complementar* de A em relação a B, indicada por $C_B(A)$. Mostre que, se $A, A' \subset B$

a) $C_B(C_B(A)) = A$

b) Se $C_B(A') \subset C_B(A)$ então $A \subset A'$

c) $C_B(A \cap A') = C_B(A) \cup C_B(A')$

1.15. Sejam A e B dois conjuntos e f uma função de A em B. Se X é um subconjunto de A a *imagem direta de X pela função f* é o conjunto $f(X) = \{y \in B | \ y = f(x)$ para algum $x \in A\}$. Seja Y outro subconjunto de A. Mostre que

a) Se $X \subset Y$ então $f(X) \subset f(Y)$

b) $f(X \cup Y) = f(X) \cup f(Y)$

c) $f(X \cap Y) \subset f(X) \cap f(Y)$

d) Encontre um contraexemplo que mostre que $f(X \cap Y) \neq f(X) \cap f(Y)$

e) $f(X - Y) \supset f(X) - f(Y)$

f) Encontre um contraexemplo que mostre que $f(X - Y) \neq f(X) - f(Y)$

1.16. Sejam A e B dois conjuntos e f uma função de A em B. Se Y é um subconjunto de B a *imagem inversa* de Y pela função f é o conjunto $f^{-1}(Y) = \{x \in A | \ f(x) \in Y\}$. Seja Z outro subconjunto de A. Mostre que

a) Se $Y \subset Z$ então $f^{-1}(Y) \subset f^{-1}(Z)$

b) $f^{-1}(Z \cup Y) = f^{-1}(Z) \cup f^{-1}(Y)$

c) $f^{-1}(Z \cap Y) = f^{-1}(Z) \cap f^{-1}(Y)$

d) $f^{-1}(X - Y) = f^{-1}(X) - f^{-1}(Y)$

1.17. 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

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

1.19. Sejam A e B dois conjuntos e f uma função de A em B. Mostre que existe uma função g, de B em A, tal que $f \circ g = I_B$ se e somente se f é sobrejetiva. Neste caso, a função g é dita *inversa à direita* de f.

1.20. Sejam A e B dois conjuntos e f uma função de A em B. Mostre que existe uma função g, de B em A, tal que $g \circ f = I_A$ se e somente se f é injetora. Neste caso, a função g é dita *inversa à esquerda* de f.

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 que uma *função* não o é, sendo definida como o foi na seção 1.10.

Uma outra forma de se conceber um objeto matemático é se estabelecer propriedades às quais ele deve satisfazer, independentemente de qualquer conceituação anterior. Neste caso, tais propriedades são chamadas *axiomas* ou *postulados* e diz-se 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*) a que estes 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 definições ou construções axiomáticas) a serem manipulados na teoria e do estabelecimento de propriedades gozadas pelos entes primitivos e pelos novos objetos definidos. Estas 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 utilizando-os 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 aos 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) $p(1) = V$,

   ii) se $p(n) = V$, então $p(s(n)) = V$,

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 temos $s(n) \neq n$, 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 este axioma implica que todo elemento $n \in \mathbb{N}$, $n \neq 1$, é sucessor de um natural m. Este 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* 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* pode ser enunciado de uma outra forma.

Proposição 1.2

O princípio da indução 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 implica a propriedade acima. Para isto, 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 $p(x) = V$ se e somente se $x \in A$. De $1 \in A$ temos que $p(1) = V$ e de $n \in A$ implica $s(n) \in A$ temos que $p(n) = V$ implica $p(s(n)) = V$. 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. Seja então um predicado p em $\mathbb{N}$ tal que $p(1) = V$ e se $p(k) = V$, então $p(s(k)) = V$. Considere o conjunto $A = \{x \in \mathbb{N} \mid p\}$. De $p(1) = V$ segue que $1 \in A$ e de $p(k) = V$ implica $p(s(k)) = V$ 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

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

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

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

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 $n \cdot s(m) = n \cdot m + n$.

É necessário se provar que estas 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 $n \cdot m \in \mathbb{N}$. 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 $\mathbb{N}$. Evidentemente, este raciocínio pode se aplicar 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 $2 = 1 + 1$ 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 estas 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. Neste caso, n e m são chamados *parcelas*. A imagem $n \cdot m$ é chamada *produto* de n por m. Neste caso, n e m são chamados *fatores*. Um produto do tipo $n \cdot n$ pode ser representada por n^2 (lido *n ao quadrado*).

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 multiplicação, necessitamos do seguinte lema.

Lema 1.2

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

i) $n + 1 = 1 + n$;
ii) $n \cdot 1 = 1 \cdot n$.

Demonstração

i) Consideremos o predicado em $\mathbb{N}$

$$p(n) = V \text{ se } n + 1 = 1 + n.$$

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, $p(n) = V$ para todo $n \in \mathbb{N}$.

ii) Consideremos o predicado em $\mathbb{N}$,

$$p(n) = V \text{ se } n \cdot 1 = 1 \cdot n.$$

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) $n \cdot (m + p) = n \cdot m + n \cdot p$ (distributividade da multiplicação em relação à adição);
iii) $n \cdot (m \cdot p) = (n \cdot m) \cdot p$ (associatividade da multiplicação);
iv) $n + m = m + n$ (comutatividade da adição);
v) $n \cdot m = m \cdot n$ (comutatividade da multiplicação);

Demonstração.

i) Sejam $n, m \in \mathbb{N}$ e consideremos o predicado em $\mathbb{N}$

$$p(k) = V \text{ se } (n + m) + k = n + (m + k).$$

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

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

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

ii) Sejam $n, m \in \mathbb{N}$ e consideremos o predicado em $\mathbb{N}$

$$p(k) = V \text{ se } n \cdot (m + k) = n \cdot m + n \cdot k.$$

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

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

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

iii) Sejam $n, m \in \mathbb{N}$ e consideremos o predicado em $\mathbb{N}$

$$p(k) = V \text{ se } (n \cdot m) \cdot k = n \cdot (m \cdot k).$$

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

Suponhamos que $p(k) = V$, ou seja, suponhamos que $(n \cdot m) \cdot k = n \cdot (m \cdot k)$, e provemos que $p(s(k)) = V$. Temos

$(n \cdot m) \cdot s(k) = (n \cdot m) \cdot k + (n \cdot m)$	(definição da multiplicação)
$(n \cdot m) \cdot s(k) = n \cdot (m \cdot k) + n \cdot m$	(hipótese indutiva)
$(n \cdot m) \cdot s(k) = n \cdot (m \cdot k + m)$	(distributividade "ao contrário")
$(n \cdot m) \cdot s(k) = n \cdot (m \cdot s(k))$	(definição de 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

$n + s(m) = n + (m + 1)$	(definição de sucessor)

$n + s(m) = (n + m) + 1$	(associatividade da adição)
$n + s(m) = (m + n) + 1$	(hipótese indutiva)
$n + s(m) = m + (n + 1)$	(associatividade da adição)
$n + s(m) = m + (1 + n)$	(lema 1.2)
$n + s(m) = (m + 1) + n$	(associatividade da adição)
$n + s(m) = s(m) + n$	(definição de sucessor)

v) 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 $p(s(m)) = V$.

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

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

$(m + n) \,.\, (k + 1) = (m + n) \,.\, k + m + n$	(distributividade e associatividade da soma)
$(m + n) \,.\, (k + 1) = m \,.\, k + n \,.\, k + m + n$	(hipótese indutiva)
$(m + n) \,.\, (k + 1) = m \,.\, k + m + n \,.\, k + n$	(comutatividade da adição)
$(m + n) \,.\, (k + 1) = m \,.\, (k + 1) + n \,.\, (k + 1)$	(distributividade "ao contrário")

Agora, voltando ao predicado p, temos

$n \,.\, (m + 1) = n \,.\, m + n$	(definição de multiplicação)
$n \,.\, (m + 1) = m \,.\, n + n$	(hipótese indutiva)
$n \,.\, (m + 1) = m \,.\, n + 1 \,.\, n$	$(n = n \,.\, 1 = 1 \,.n)$
$n \,.\, (m + 1) = (m + 1) \,.\, n$	(demonstração acima)

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

$3 + 4 = 4 + 3 = 4 + (2 + 1) = 4 + (1 + 2) = (4 + 1) + 2 = 5 + 2 = 5 + (1 + 1) = 6 + 1 = 7$
$2 \,.\, 4 = 2 \,.\, (2 + 2) = 2 \,.\, 2 + 2 \,.\, 2 = 4 + 4 = 4 + (3 + 1) = (4 + 3) + 1 = 7 + 1 = 8.$

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 $n \,.\, (m + p) = n \,.\, m + n \,.\, p$, foi algumas vezes utilizada do segundo membro para o primeiro. Quando se utiliza esta propriedade neste 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 que $m \,.\, n = (1 + 1 + \ldots + 1) \,.\, n = n + n + \ldots + n$, 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 $s(n) + m = (n + 1) + m = n + (1 + m) = n + (m + 1) = n + s(m)$.

Observe que a injetividade da função *sucessor*, estabelecida no primeiro axioma de Peano, implica que $n + 1 = m + 1$ acarreta $m = n$. Na verdade, esta 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, 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, $s(n) + (k - 1) = m$. Esta 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 $n + k = n$. Desta 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 $n \cdot p = m \cdot p$, 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 $(n + r) \cdot p = m \cdot p$ o que implicaria $n \cdot p + r \cdot p = m \cdot p$ e a equação $n \cdot p + x = m \cdot p$ seria solúvel, contrariando o item i da proposição anterior, pois, por hipótese, $n \cdot p = m \cdot p$. Como é evidente que este 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 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. Logo $a = b$ 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 às 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 $n \cdot p \leq m \cdot p$.

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 $n \,.\, p = m \,.\, p$. De $n + r = m$ segue que $n + (\mathrm{r} + p) = m + p$ e $n \,.\, p + \mathrm{r} \,.\, p = m \,.\, p$, que implicam $(n + p) + \mathrm{r} = m + p$ e $n \,.\, p + \mathrm{r} \,.\, p = m \,.\, p$. Logo, $n + p \leq m + p$ e $n \,.\, p \leq m \,.\, p$.

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 $n + \mathrm{x} = m$ é solúvel" são incompatíveis, dizer que $n < m$ implica que a equação $n + \mathrm{x} = m$ é solúvel. Ou seja, $n < m$ se e somente se existe um natural r tal que $n + r = m$. Observe que $<$ pode ser vista como uma relação binária em $\mathbb{N}$que, como é fácil provar, 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 contrariam o segundo axioma de Peano.

O conjunto dos números naturais satisfaz a 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 imediato 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 $n < \mathrm{s}(m)$.

Observe que o item ii desta 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))

Seja M um subconjunto dos números naturais. Se $M \neq \emptyset$, então existe $p \in M$ tal que $p \leq m$ qualquer que seja $m \in M$.

Demonstração

Consideremos o conjunto $L = \{x \in \mathbb{N} \mid m \in M \Rightarrow x \leq m\}$. Observe que o item (i) do lema anterior implica que $1 \in L$. Além disso, como pelo item (ii) do lema anterior $s(k) > k$, 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 do lema 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 $I_n = \{x \in \mathbb{N} \mid x \leq n\}$. Dizemos que um conjunto A é *finito* se $A = \emptyset$ 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 $Y = \{x \in \mathbb{N} \mid$ existem $A \subset I_x$, $A \neq I_x$, e uma bijeção f de A em $I_x\}$. Devemos provar que $Y = \emptyset$. Por contradição, suponhamos que $Y \neq \emptyset$. 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 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 ∘ 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, $A \cap B = \varnothing$), $|A \cup B| = |A| + |B|$ (ver exercício 2.11). Este 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 num 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

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 $\mathbb{N}$:

$p(n)$ = V se n é número pequeno.

Temos que $p(1)$ = V, pois 1 é um numero pequeno. Além disto, se $p(n)$ = V, é óbvio que $p(s(n))$ = 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 esta "demonstração"?.

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

a) $2 \cdot a = a + a$.

b) $(a + b)^2 = a^2 + 2 \cdot a \cdot b + b^2$.

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

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

a) $1 + 3 + ... + (2 . n – 1) = n^2$.

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

2.6. Em $\mathbb{N}$ definamos a operação $n \otimes m = n + m + n . m$. 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. Mostre que

a) $n – m = (n + p) – (m + p)$.

b) Se $n – m = p$, então $n – p = m$.

c) $(n – m) . p = n . p – m . p$.

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 $a . c < b . c$.

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

2.10. Mostre que se k e j são números naturais tais que k . j = 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 $a = b . q$".

Mostre que esta 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 e B dois conjuntos nfinitos e não vazio. Mostre que |AxB| = |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 $n < m$. 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 este débito em relação ao saldo da sua mesada? Para que possamos fazer isto é necessário "ampliarmos" o conjunto dos números naturais, obtendo então o 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. Esta 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, nesta construção, o Princípio da Indução Matemática agora será um teorema enquanto que o Princípio da Boa Ordenação será um axioma, ao contrário da construção axiomática dos números naturais. Esta 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. Uma *estrutura algébrica* consiste de um conjunto munido de uma ou mais operações que gozem de propriedades preestabelecidas. Estudaremos os *anéis* e outras "estruturas derivadas".

3.2 Anéis

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

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

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

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

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

(M_1) A multiplicação é associativa: $a \,.\, (b \,.\, c) = (a \,.\, b) \,.\, c$, quaisquer que sejam $a, b, c \in A$.

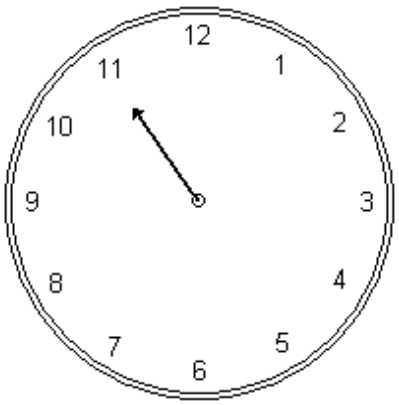
(M_2) A multiplicação é comutativa: $a \,.\, b = b \,.\, a$, quaisquer que sejam $a, b \in A$.

(M_3) A multiplicação possui elemento neutro: existe $f \in A$, $f \neq e$, tal que $a \,.\, f = a$, qualquer que seja $a \in A$.

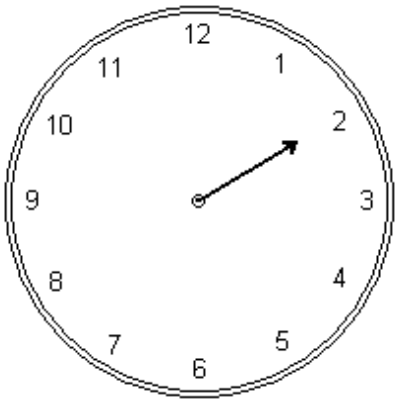
(AM) A multiplicação é distributiva em relação à adição: $a \,.\, (b + c) = a \,.\, b + a \,.\, c$, quaisquer que sejam $a, b, c \in A$.

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*).

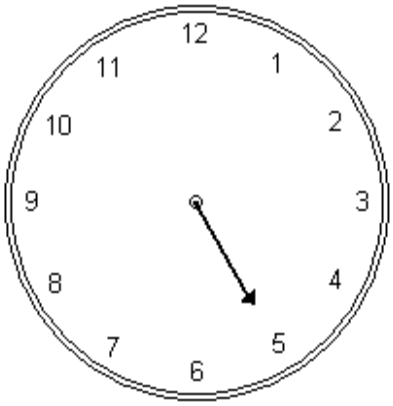
Consideremos, para exemplificar, um mostrador de um relógio.
Imagine que num determinado instante o ponteiro das horas esteja sobre a marca das 11 horas.



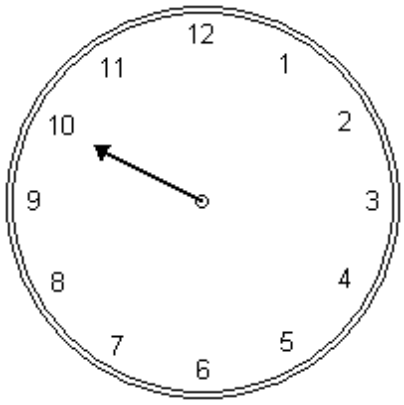
Três horas após esse instante, o ponteiro estará sobre a marca das 2 horas;



seis horas após aquele instante o ponteiro estará sobre a marca das 5 horas



e 11 horas após, ele estará sobre a das 10 horas.



De forma natural, podemos expressar estes 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 $3 \cdot 7 = 9$.

Isto mostra que, de forma natural, pode-se 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

Naturalmente, o leitor está pensando que é muito complicado executar estas operações. No capítulo 7 apresentaremos uma forma simples de realizá-las.

Por enquanto, o leitor precisa observar apenas que $a + 12 = a$, para todo $a \in I_{12}$, o que mostra que 12 é elemento neutro da adição. Precisa observar também que $a \,.\, 1 = a$, 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 estas 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, estas demonstrações são simples e serão feitas, num caso mais geral, no capítulo 7. Por ora, observe (lembrando que isto não é uma demonstração, são apenas exemplos!) 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

$$5 \,.\, (7 + 3) = 5 \,.\, 10 = 2,$$
$$5 \,.\, 7 + 5 \,.\, 3 = 11 + 3 = 2.$$

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 destas operações é um *anel*.

Para um outro exemplo, considere os dias da semana, associando os naturais 1, 2, 3, 4, 5, 6 e 7 aos dias domingo, segunda-feira, terça-feira, quarta-feira, quinta-feira, sexta-feira e sábado, respectivamente. Como se sabe, se estivermos numa quinta-feira, após o decurso de seis dias iremos para uma quarta-feira. Isto poderia ser expresso por $5 + 6 = 4$; do mesmo modo, se estivermos num domingo e forem decorridos sete dias iremos para um outro domingo. Ou seja, $1 + 7 = 1$. De forma semelhante, decorridos três vezes o período de quatro dias, a partir do domingo, iremos parar numa quinta-feira (o primeiro período terminaria numa quarta-feira, o segundo terminaria num domingo e, então, o terceiro acabaria numa quinta-feira). Assim, $3 \,.\, 4 = 5$.

Desta forma, estabelecemos duas operações no conjunto $I_7 = \{1, 2, 3, 4, 5, 6, 7\}$.

Adição em I_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	1	2	3	4	5	6	7

Multiplicação em I_7

.	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

Do mesmo modo que o I_{12}, o conjunto I_7 munido das operações acima é um anel. O conjunto dos naturais não é um anel pelo fato de que não existe elemento neutro para adição.

O elemento neutro (único, como mostrado na seção 1.12) 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 $12 = 0$; em I_7, $7 = 0$. 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. 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. 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*. 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 desta 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 $a \cdot 0 = 0$.

Demonstração:

Temos

$a \cdot 0 = a \cdot (0 + 0)$	$(0 = 0 + 0)$
$a \cdot 0 = a \cdot 0 + a \cdot 0$	(distributividade da multiplicação)
$a \cdot 0 = 0$	(observação anterior: se $k + k = k$, então $k = 0$)

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

Proposição 2.3

Seja A um anel. Para todos $a, b \in A$,
a) $(-1) \cdot a = -a$.
b) $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$.
c) $(-a) \cdot (-b) = a \cdot b$.

Demonstração:

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

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

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

b) Temos $(-a) \cdot b = ((-1) \cdot a) \cdot b = (-1) \cdot (a \cdot b) = -(a \cdot b)$. Para a outra igualdade, temos $a \cdot (-b) = (-b) \cdot a$ e, então, $a \cdot (-b) = -(b \cdot a) = -(a \cdot b)$.

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

$$(-a) \cdot (-b) = -(a \cdot (-b)) = -(-(a \cdot b)) = a \cdot b$$

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 $a \cdot b = 1$. Neste caso dizemos que a é *inversível* e b é chamado *inverso* de a. Como mostrado no capítulo primeiro, o inverso de um elemento inversível a é único e será 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 I_7, todos os elementos não nulos são inversíveis, sendo, por exemplo, $2^{-1} = 4$ e $3^{-1} = 5$.

Devido ao fato de que $a \cdot 0 = 0$, 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 $1 \cdot 1 = 1$, o elemento neutro da multiplicação é sempre inversível e $1^{-1} = 1$. Como o item (c) da proposição 2.3 mostra que $(-1) \cdot (-1) = 1 \cdot 1$, 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 deste 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 esta definição vá ao encontro da lógica do senso comum. É fácil aceitar que não havia sentido uma definição de igualdade de anéis que tornasse iguais os anéis I_{12} e I_7. 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, em consequência, da preservação das operações respectivas em relação aos objetos e suas imagens. Ou seja, é razoável esperar que dois anéis $(A, +, .)$ e $(B, \#, *)$ serão iguais se existir uma função bijetiva f de A em B que satisfaça às seguintes propriedades:

a) $f(a + b) = f(a) \# f(b)$.
b) $f(a \cdot b) = f(a) * f(b)$.
c) $f(1_A) = 1_B$.
d) $f(0_A) = 0_B$.
e) $f(a - b) = f(a) \sim f(b)$, com $\sim$ indicando a subtração em B.
f) $f(-a) = \sim f(a)$.

É interessante observar que, como mostra a proposição a seguir, os itens d, e, e f da observação acima são corolários dos itens a, b e c.

Proposição 3.3.

Sejam $(A, +, .)$ e $(B, \#, *)$ dois anéis e f uma função de A em B tal que $f(a + b) = f(a) \# f(b)$, $f(a \cdot b) = f(a) * f(b)$ e $f(1_A) = 1_B$. 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 $f(a - b) = f(a + (-b)) = f(a) \# f(-b) = f(a) \sim f(b)$.

De um modo geral, se E e F são duas estruturas algébricas de um mesmo tipo, uma função bijetiva de E em F que preserve as operações das estruturas é chamada de *isomorfismo de E em F*. A proposição acima afirma que para que uma função bijetiva f de um anel $(A, +, .)$ num anel $(B, \#, *)$ seja um isomorfismo de A em B basta que $f(a + b) = f(a) \# f(b)$, $f(a . b) = f(a) * f(b)$ e $f(1_A) = 1_B$ (caso em que f é dita um *homomorfismo* do anel A no anel B).

A proposição a seguir mostra que a função inversa de um isomorfismo é também um isomorfismo, o que nos permite falar em *anéis isomorfos*.

Proposição 4.3

Sejam os anéis $(A, +, .)$ e $(B, \#, *)$. Se a função f é um isomorfismo de A em B, então a função inversa de f 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, $f^{-1}(c \# d) = f^{-1}(c) + f^{-1}(d)$.

Claramente, a igualdade $f^{-1}(c * d) = f^{-1}(c) . f^{-1}(d)$ se demonstra de forma semelhante. 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, se dois anéis são isomorfos há uma correspondência biunívoca entre os dois conjuntos que preserva as operações "nos dois sentidos". Assim, 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 esta razão, a existência de um isomorfismo entre dois anéis é utilizado para definir igualdade de dois anéis: *dois anéis são iguais quando eles são isomorfos*.

3.5 Domínios de integridade

Se o leitor observar a tabela de multiplicação do anel I_{12} e se lembrar que neste anel $12 = 0$, verificará, ao contrário do que estamos habituados, que $3 . 8 = 0$. Ou seja, o *produto* de dois elementos não nulos é igual a zero! Observe que tal fato não ocorre no anel I_7.

Um anel em que este fato não acontece é chamado *domínio de integridade*, que pode ser formalmente definido da seguinte forma.

Seja A um anel. Diz-se que A é um *domínio de integridade* se a multiplicação do anel satisfizer à seguinte propriedade.

(M_4) Quaisquer que sejam $a, b \in A$, se $a . b = 0$, 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 I_7 é um domínio de integridade.

Claramente, a propriedade (M_4) acima é equivalente à seguinte propriedade.

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

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 $a \,.\, b = a \,.\, c$, então $b = c$.

Demonstração

De $a \,.\, b = a \,.\, c$ segue que $a \,.\, b + (-a \,.\, c) = 0$ o que implica $a \,.\, b + (a \,.\, (-c)) = 0$. 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 $a \,.\, b = a \,.\, c$ (se $a \neq 0$) obtendo $b = c$, dizemos que *dividimos* a igualdade $a \,.\, b = a \,.\, c$ por a ou que a igualdade $a \,.\, b = a \,.\, c$ foi *simplificada* por a.

3.6 Anéis ordenados

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 às 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 $a \,.\, c \leq b \,.\, c$.

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 solução facílima) mostrará que $x < y$ é também transitiva. Assim podemos usar $x < y < z$ para indicar que $x < y$ e $y < z$. Neste 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 às propriedades abaixo, que, combinadas com as propriedades estabelecidas na proposição 2.3, são conhecidas como *regra 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 $a \,.\, b \geq 0$.
d) Se $a \geq 0$ e $b \leq 0$, então $a \,.\, b \leq 0$.
e) Se $a \leq 0$ e $b \leq 0$, então $a \,.\, b \geq 0$.

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 $a \,.\, b \geq 0 \,.\, b$ 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 $b \,.\, a \leq 0 \,.\, a$.

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, $-(b \,.\, a) \leq 0$. Aplicando agora o item (*b*), $-(-(b \,.\, a)) \geq 0$ e, portanto, $b \,.\, a \geq 0$.

Para estabelecer a igualdade entre dois anéis ordenados, diremos que dois anéis ordenados A e B são *isomorfos como anéis ordenados* se existe um isomorfismo f de A em B tal que, para todos $a, b \in A$, $a \leq b$ implicar $f(a) \leq f(b)$. Assim, estendendo naturalmente o conceito de igualdade de anéis, dois anéis ordenados são iguais se eles são isomorfos como anéis ordenados.

3.7 Domínios bem ordenados

Falta pouco para a caracterização axiomática dos números inteiros. Para isto, há a necessidade de mais algumas definições. Seja A um anel ordenado. Um subconjunto S do anel 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 $x \geq a$.

Diz-se que o subconjunto S 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 este 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, $b' = b''$.

Um domínio de integridade ordenado A é dito *domínio bem ordenado* se satisfizer à seguinte propriedade.

Princípio da Boa Ordenação (PBO)

Todo subconjunto não vazio 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 isto necessitamos discutir uma propriedade importante de predicados definidos em domínios bem ordenados. Como veremos, esta propriedade se assemelha ao terceiro postulado de Peano e, por esta 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 0 e 1.

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 $S = \varnothing$. Se $S \neq \varnothing$, 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 esta 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 desta propriedade o fato de que, num domínio bem ordenado, não

existe elemento entre dois elementos do tipo y e $y + 1$.

Corolário 1.3

Num 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, $x \geq y + 1$.

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

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

Demonstração

Basta provar que o conjunto $S = \{z \in D | z \geq k$ e $p(z) = F\}$ é vazio. Suponhamos $S \neq \varnothing$. 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.

3.8 O conjunto dos números inteiros

Mostraremos nesta seção que todos os domínios bem ordenados são isomorfos como anéis ordenados. Isto 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 $\mathbb{Z}$, tirado 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, a um elemento de A, $(D, \#, *)$ um domínio bem ordenado 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

$$z \times a = \begin{cases} a + (z \sim 1) \times a, & se\ z > 0_d \\ 0_a, se\ z = 0_d \\ -\big((\sim z) \times a\big), se\ z < 0_d \end{cases}$$

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

$1_D \times a = a + (1_D \sim 1_D) \times a = a + 0_D \times a = a + 0_A = a.$
$2_D \times a = a + (2_D \sim 1_D) \times a = a + 1_D \times a = a + a = 2_A.$

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) $m \times (a \,.\, b) = (m \times a) \,.\, b$.

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

$(m \# (n \# 1_D)) \times a = a + ((m \# (n \# 1_D) \sim 1_D) \times a)$	(definição)
$(m \# (n \# 1_D)) \times a = a + ((m \# n) \times a)$	$(1_D \sim 1_D = 0_D)$
$(m \# (n \# 1_D)) \times a = a + (m \times a) + (n \times a)$	(hipótese de indução)
$(m \# (n \# 1_D)) \times a = (m \times a) + (n \times a) + a$	(comutatividade)
$(m \# (n \# 1_D)) \times a = (m \times a) + ((n \# 1_D) \times a)$	(base de indução).

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, $(m \# n) \times a = -((\sim m) \times a) - ((\sim n) \times a)) = -(-(m \times a) - (-(n \times a)) = ma + na$, 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

$(m \# 1_D) \times (a + b) = (m \times (a + b)) + (1_D \times (a + b))$	(item b)
$(m \# 1_D) \times (a + b) = (m \times a) + (m \times b) + a + b$	(hipótese indutiva e exemplo acima)

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

Para $m < 0_D$,

$m \times (a + b) = -((\sim m) \times (a + b))$	(definição)
$m \times (a + b) = -(((-m) \times a) + ((-m) \times b))$	$(-m > 0_D)$
$m \times (a + b) = -((\sim m) \times a) + (-((-m) \times b)$	(distributividade no anel)
$m \times (a + b) = (m \times a) + (m \times b)$	(definição)

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

$(m * (n \# 1_D)) \times a = ((m * n) \# m) \times a$	(distributividade no domínio)
$(m * (n \# 1_D)) \times a = ((m * n) \times a) + (m \times a)$	(item *b*)
$(m * (n \# 1_D)) \times a = m \times (n \times a) + (m \times a)$	(hipótese de indução)
$(m * (n \# 1_D)) \times a = m \times ((n \times a) + a)$	(item c)
$(m * (n \# 1_D)) \times a = m \times ((n \# 1_D) \times a)$	(item b)

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 $m * n < 0_D$,

$(m * n) \times a = -((\sim(m * n)) \times a)$	(definição)
$(m * n) \times a = -(((\sim m) * n) \times a)$	$(-(m * n) = (-m) * n)$
$(m * n) \times a = -((\sim m) \times (n \times a))$	$((-m) \,.\, n > 0)$
$(m * n) \times a = -(-(m \times (n \times a)))$	(item a)
$(m * n) \times a = m \times (n \times a)$	(-(-x) = x no anel).

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

$(m + 1_D) \times (a \,.\, b) = m \times (a \,.\, b) + a \,.\, b$	(item *b*)
$(m + 1_D) \times (a \,.\, b) = (m \times a) \,.\, b + a \,.\, b$	(hipótese indutiva)
$(m + 1_D) \times (a \,.\, b) = (m \times a + a) \,.\, b$	(distributividade no anel)
$(m + 1_D) \times (a \,.\, b) = ((m \# 1_D) \times a) \,.\, b$	(item b)

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

Corolário 2.3

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

Demonstração

Temos $(m * n) \times (a \,.\, b) = m \times (n \times (a \,.\, b)) = (m \times (n \times a)) \,.\, b = m \times ((n \times a) \,.\, b) = m \times (n \times (a \,.\, b)) = m \times (n \times (b \,.\, a)) = m \times ((n \times b) \,.\, a) = m \times (a \,.\, (n \times b)) = (m \times a) \,.\, (n \times$

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) $\rho(z_1 * z_2) = (z_1 * z_2) \times 1_D = (z_1 \times 1_D) \,.\, (z_1 \times 1_D) = \rho(z_1) \,.\, \rho(z_2)$, 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 sobrejetivo. Para tal devemos provar que todo elemento $a \in D$ é da forma $z \times 1_D$ para algum $z \in E$. Suponhamos por contradição que existe $a \in D$ tal que $a \neq z \times 1_D$, para todo $z \in$ E e consideremos os conjuntos

$$A' = \{z \times 1_D \in D \mid z \in E \text{ e } z \times 1_D > a\}$$

e

$$A'' = \{z \times 1_D \in D \mid z \in E \text{ e } z \times 1_D < a\}.$$

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 última 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 sobrejetivo.

Para provar que ρ é injetivo (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 das números inteiros satisfaz a 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 desta 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

$$|z| = \begin{cases} z, se\ z \geq 0 \\ -z, z < 0 \end{cases}$$

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) $|z \,.\, y| = |z| \,.\, |y|$.
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 desta 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 $z \,.\, y \geq 0$ e a igualdade a ser provada decorre da definição.

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

$\|z \,.\, y\| = -(z \,.\, y)$	(definição de valor absoluto)
$\|z \,.\, y\| = z \,.\, (-y)$	(item (b) da proposição 2.3)
$\|z \,.\, y\| = \|z\| \,.\, \|y\|$	(definição de valor absoluto

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

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

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 $|z \cdot y| \geq |z|$.

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 $|z| \cdot |y| \geq |z| \cdot 1$ 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 $n \cdot y \geq z$.

Demonstração

Pelo corolário anterior temos $|z \cdot y| \geq |z|$ e então $|y| \cdot |z| \geq |z|$ que implica $|y| \cdot |z| \geq z$, 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 $z \cdot y = 1$. 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 $|z \cdot y| \geq |z|$ e, portanto, $|z| \leq 1$, pois $|z \cdot y| = 1$. 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. Como vimos no exercício 2.7, uma *sequência* 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 $x_n = f(n)$. Num 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) de inteiros tal que $x_1 > x_2 > x_3 > ... > x_n > ... > 0$, 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*, 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

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

3.1 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 $b = 0$.

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

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

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

3.3 Mostre que dois elementos a e b de um anel são inversíveis se e somente se $a \,.\, b$ é inversível.

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 $\cdot$ ao conjunto $A' \times A'$).

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 $a \,.\, b \in A'$ quaisquer que sejam $a, b \in A$

b) Sejam A e B dois anéis e f um homomorfismo de A em 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 conjunto não vazio e $\mathfrak{I}(A)$ o conjunto das funções de A em A. Dadas f, 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 da operação definida acima 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 $a \,.\, b = a$ 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 $f_a(x) = a \,.\, x$.

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 $a \,.\, c \geq b \,.\, c$.

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 $a \,.\, c < b \,.\, c$.

b) Se $a \,.\, c \leq b \,.\, c$ e $c > 0$, então $a \leq b$.

c) Se $a \,.\, c \leq b \,.\, c$ 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 $a^2 = a \,.\, b$ donde se conclui, somando a ambos os termos $a^2 - 2 \,.\, a \,.\, b$, a igualdade

$$a^2 + a^2 - 2 \,.\, a \,.\, b = a^2 - 2 \,.\, a \,.\, b + a \,.\, b.$$

Daí,

$$2 \,.\, a^2 - 2 \,.\, a \,.\, b = a^2 - a \,.\, b,$$

e, então,

$$2 \,.\, (a^2 - a \,.\, b) = 1 \,.\, (a^2 - a \,.\, b).$$

Pela lei do cancelamento,

$$2 = 1.$$

Evidentemente, esta "demonstração" está errada! Verifique qual o erro cometido na "demonstração" acima.

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* pela seguinte igualdade.

$$z^n = \begin{cases} 1, se\ n = 0 \\ z \,.\, z^{n-1}, se\ n > 0 \end{cases}$$

Mostre que para todos $a, b, m, n \in \mathbb{Z}$ com $a, b \neq 0$ e $m, n \geq 0$ temos

a) $a^m \,.\, b^m = (a \,.\, b)^m$.

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) $a^2 - a \,.\, b + b^2 \geq 0$.

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. Uma *sequência* (ou uma *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 $x_n = f(n)$. Neste caso, a expressão que identifica x_n é chamada *termo geral* da sequência.

a) Represente a sequência de números inteiros cujo termo geral é $x_n = 2 \,.\, n - 1$.

b) 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, nestas condições, o termo geral de uma PA é dado por $x_n = x_1 + (n - 1) \,.\, r$.

3.19. 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, nestas condições, o termo geral de uma PG é dado por $x_n = x_1 \,.\, q^{(n-1)}$.

3.20. Sejam a, b e n números inteiros, com $n > 1$. Mostre que

$$a^n - b^n = (a - b) \,.\, (a^{n-1} + a^{n-2} \,.\, b + a^{n-3} \,.\, b^2 + \ldots + a \,.\, b^{n-2} + b^{n-1}).$$

3.21. Seja $\frac{z}{2}$ o número inteiro y (se existir) tal que $2 \,.\, y = z$. Considerando as condições de existência, mostre que, $\frac{z}{2} + w = \frac{z + 2 \,.\, w}{2}$.

3.22. Mostre que, para todo inteiro $z \geq 1$, $1 + 2 + ... + z = \frac{z \,.\, (z+1)}{2}$.

3.23. Mostre que, para todo inteiro $k \geq 0$, $1 + 2 + 4 + ... + 2^k = 2^{k+1} - 1$.

3.24. Dados $n \in \mathbb{Z}, n \geq 0$, definimos o *fatorial de n* por

$$n! = \begin{cases} 1, se\ n\ 0\ ou\ n = 1 \\ n \,.\, (n-1)!, se\ n > 1 \end{cases}$$

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 $(1 + z)^n \geq 1 + n \,.\, z$, 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 numa 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 este 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) para $n \geq 2$, $a_n = 2a_{n-1} + 1$.

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 $\mathbb{Z} \times \mathbb{Z}^*$ a relação $(a, b) \approx (c, d)$ se $a \cdot d = b \cdot c$. Mostre que $\approx$ é uma relação de equivalência.

3.29. Considere a operação $(a, b) \# (c, d) = (a \cdot c - b \cdot d, a \cdot d + b \cdot c)$ definida no conjunto $\mathbb{Z} \times \mathbb{Z}^*$ da questão anterior, com $+$, $\cdot$ e $-$ sendo as operações em $\mathbb{Z}$ Mostre que a operação # 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 destes elementos, 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 à determinada propriedade. A ideia é a seguinte: para se provar que existe um inteiro que satisfaça a uma propriedade específica apresenta-se uma "receita" de como encontrar tal inteiro. Em matemática e ciência da computação, uma "receita" com este 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 fogem do objetivo 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 a 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 num intervalo de tempo finito, 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 desta 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 isto, 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*, o valor -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

Neste 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 Media de três números;
    leia(x, y, z);
    media := (x + y + z)/3;
    escreva(media);

2. Naturalmente, a extensão do algoritmo acima para o cálculo da média de muitos números

(5 000, 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 isto utiliza-se uma outra variável que vai armazenado as somas parciais, recebendo esta 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;
    média := soma/n;
    escreva(média);
```

3. O algoritmo abaixo calcula a *potência* a^n, *a* e *n* dados, definição dada no exercício 3.16.

```
algoritmo Potência;
    leia(a, n);
    potência := 1;
    se n > 0
        então
            repita n vezes
                potência := potência . a;
    escreva(potência);
```

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 no exercício 3.21.

```
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 esta e o menor dos números for digitado inicialmente nada precisa ser feito; se isto 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 (http://mathworld.wolfran.com/CollatzProblem.html, acessado em 11/02/2010) se ela constitui um algoritmo. Como foi dito acima, 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* se encontra no exercício 5.7).

```
algoritmo (?) de Collatz
    leia(z);
    repita enquanto z > 1
        se z é ímpar
            então
                z := 3 . z + 1
            senão
                z := z/2;
    escreva(z);
```

Este é um dos problemas de Matemática que ainda não tem solução, embora todos os matemáticos concordam que, de fato, se trata de uma algoritmo. Tomás Oliveira e Silva, da Universidade de Aveiro, Portugal, executou (num computador, é claro) este algoritmo para todos os inteiros menores que $19 \cdot 2^{55}$ e não encontrou nenhum contraexemplo.

4.3 Exercícios

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 retorne 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.

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 $a = b \cdot q$.

Por exemplo, $1|2$ pois $2 = 1 \cdot 2$; como 2 não é inversível, não existe inteiro q tal que $1 = 2 \cdot q$ e, portanto, $\sim(2|1)$ (ou $2 \not| 1$). Este 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*. Neste caso, o inteiro q tal que $a = b \cdot q$ 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 $n = m \cdot q_1$ e $p = n \cdot q_2$. Daí, $p = (m \cdot q_1) \cdot q_2 = m \cdot (q_1 \cdot q_2)$ 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 $n = m \cdot q_1$ e $m = n \cdot q_2$. Daí, $n = (n \cdot q_2) \cdot q_1$ o que implica $n = n \cdot (q_1 \cdot q_2)$. Se $n = 0$, temos $m = 0$ e então $m = n$. Se $n \neq 0$, pela lei do corte, $1 = q_1 \cdot q_2$ 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

Sejam os inteiros a, b, c, d, a_1, ..., a_n. Temos que

a) Se $b|a$ e $d|c$, então $(b \cdot d)|(a \cdot c)$.
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 segue que existem q_1 e q_2 tais que $a = b \cdot q_1$ e $c = d \cdot q_2$. Multiplicando estas duas igualdades, $a \cdot c = (b \cdot q_1) \cdot (d \cdot q_2) = (b \cdot d) \cdot (q_1 \cdot q_2)$ e, então, $(b \cdot d)|(a \cdot c)$.
b) Da hipótese segue que existem q_1 e q_2 tais que $a + c = b \cdot q_1$ e $a = b \cdot q_2$. Dai, substituindo a

segunda na primeira, $b \cdot q_2 + c = b \cdot q_1$ o que implica $c = b \cdot (q_1 - q_2)$. Desta igualdade concluímos que $b|c$.

c) De $b|a_i$, para $i = 1, ..., n$, segue que existem q_i, $i = 1, ..., n$, tais que $a_i = b \cdot q_i$, $i = 1, ..., n$. Daí, para quaisquer os inteiros $c_1, ..., c_n$, $c_1 \cdot a_1 + ... + c_n \cdot a_n = c_1 \cdot (b \cdot q_1) + ... + c_n \cdot (b \cdot q_n)$, o que resulta em $c_1 \cdot a_1 + ... + c_n \cdot a_n = b \cdot (c_1 \cdot q_1 + ... + c_n \cdot q_n)$.

Se $a_1, ..., a_n$ são números inteiros, uma expressão do tipo $c_1 \cdot a_1 + ... + c_n \cdot a_n$, 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 que podem ser feitas são: como determinar *q* quando $b|a$? como saber quando $b \not| a$? O teorema a seguir, além de responder estas 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 $a = b \cdot q + r$ e $0 \leq r < |b|$. Além disso, os inteiros *q* e *r* que satisfazem às relações acima são únicos.

Demonstração

Pela *propriedade arquimediana* discutida no corolário 5.3, existe um inteiro *n* tal que $n \cdot (-b) \geq -a$. Isto garante que o conjunto $S = \{z \in \mathbb{Z} \mid z \geq 0 \text{ e } z = a - b \cdot n, \text{ para algum } n \in \mathbb{Z}\}$ 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 $r = a - b \cdot q$ para algum inteiro *q*. Ou seja, existem inteiros *q* e *r* tais que $a = b \cdot q + r$ 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 $a = b \cdot q + r$ segue $a = b \cdot q + r + |b| - |b|$ que implica $a = b \cdot (q \pm 1) + (r - |b|)$, onde $q \pm 1$ indica a expressão "$q + 1$ ou $q - 1$". Daí, $r - |b| = a - b \cdot (q \pm 1)$, 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 $a = b \cdot q_1 + r_1 = b \cdot q_2 + r_2$, 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 $b \cdot q_1 + r_1 = b \cdot q_2 + r_2$ temos que $b \cdot (q_1 - q_2) = r_2 - r_1$ e, como consequência da já citada proposição 8.3, $|b| \cdot |q_1 - q_2| = |r_2 - r_1|$. Assim, utilizando a desigualdade $|r_1 - r_2| < |b|$ mostrada acima, $|b| \cdot |q_1 - q_2| < |b|$ e então $|q_1 - q_2| < 1$. Daí, $|q_1 - q_2| = 0$ resultando $q_1 = q_2$. Da igualdade $b \cdot (q_1 - q_2) = r_2 - r_1$, segue $r_2 = r_1$, o que conclui a demonstração.

Na divisão euclidiana $a = b \cdot q + r$, com $0 \leq r < |b|$, *a* e *b* são, respectivamente, o *dividendo* e o *divisor* e *q* e *r* são o *quociente* e o *resto* da *divisão de a por b,* que 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 $b \not| a$.

Por exemplo, $q(7, 3) = 2$ e $r(7, 3) = 1$, pois, é fácil ver que $7 = 3 \cdot 2 + 1$. Assim, $3 \not| 7$.

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 $b \cdot q \leq a$
$\quad q := q + 1;$
$q := q - 1;$
$r := a - b \cdot q;$
escreva(q, r);

A propriedade arquimediana (corolário 5.3) nos garante que este algoritmo para, pois ela assegura a existência de um inteiro z tal que $z \cdot b > a$. A interrupção do comando de repetição ocorre na primeira vez que $b \cdot q > a$, porém o comando $q := q - 1$ faz com que se retorne à desigualdade $b \cdot q \leq a$. Do comando $r := a - b \cdot q$ segue que $a = b \cdot q + r$ e o fato de que $b \cdot q \leq a$ tem como consequência $r \geq 0$. Resta mostrar que $r < b$. Se $r \geq b$, $a - b \cdot q \geq b$ e, então, $a \geq b \cdot (q + 1)$. Mas isso é uma contradição, pois q é o maior inteiro tal que $b \cdot q \leq a$.

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 $a = b \cdot q + r$, com $0 \leq r < b$, segue que $a < b \cdot q + b$ o que implica $a < b \cdot (q + 1)$. Por redução ao absurdo, se $q < 0$, temos $q \leq -1$ e, então, $q + 1 \leq 0$. Daí e da desigualdade anterior $a < b \cdot (q + 1)$ segue $a \leq 0$, 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 $b \cdot q > q$. Daí e de $r \geq 0$, segue que $b \cdot q + r > q$ 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 $a = c_n \,.\, b^n + c_{n-1} \,.\, b^{n-1} + ... + c_1 \,.\, b + c_0$.

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 $a = b \,.\, q_0 + c_0$, $0 \leq c_0 < b$. Da mesma forma existem únicos q_1 e c_1 tais que $q_0 = b \,.\, q_1 + c_1$, $0 \leq c_1 < b$.

Seguindo este raciocínio obtemos $q_1 = b \,.\, q_2 + c_2$, $0 \leq c_2 < b$; $q_2 = b \,.\, q_3 + c_3$, $0 \leq c_3 < b$; …; $q_{n-2} = b \,.\, q_{n-1} + c_{n-1}$, $0 \leq c_{n-1} < b$; $q_{n-1} = b \,.\, q_n + c_n$, $0 \leq c_n < b$; …, 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,

$q_{n-2} = b \,.\, c_n + c_{n-1}$
$q_{n-3} = b \,.\, (b \,.\, c_n + c_{n-1}) + c_{n-2} = c_n \,.\, b^2 + c_{n-1} \,.\, b + c_{n-2}$
. . .
$a = c_n \,.\, b^n + c_{n-1} \,.\, b^{n-1} + ... + c_1 \,.\, b + c_0$

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

$5 = 2 \,.\, 2 + 1 = 2 \,.\, (2 \,.\, 1 + 0) + 1 = 1 \,.\, 2^2 + 0 \,.\, 2 + 1.$
$11 = 2 \,.\, 5 + 1 = 2 \,.\, (1 \,.\, 2^2 + 0 \,.\, 2 + 1) + 1 = 1 \,.\, 2^3 + 0 \,.\, 2^2 + 1 \,.\, 2 + 1,$

e, assim $1 \,.\, 2^3 + 0 \,.\, 2^2 + 1 \,.\, 2 + 1$ é a expansão binária de 11.

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. Dessa forma, $(324)_{10}$ é escrito, simplesmente, 324 e é a representação do inteiro $3 \cdot 10^2 + 2 \cdot 10 + 4$.

Quando a representação do número inteiro no sistema decimal tem mais de três algarismos, 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 $4 \cdot 10^6 + 3 \cdot 10^5 + 2 \cdot 10^4 + 4 \cdot 10^3 + + 5 \cdot 10^2 + 9 \cdot 10^1 + 1$.

Naturalmente, se a base b é menor do que dez, ela será 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

$323 = 5 \cdot 64 + 3$,
$64 = 5 \cdot 12 + 4$,
$12 = 5 \cdot 2 + 2$,
$2 = 5 \cdot 0 + 2$.

temos,

$64 = 5 \cdot 12 + 4 = 5 \cdot (5 \cdot 2 + 2) + 4 = 2 \cdot 5^2 + 2 \cdot 5 + 4$,
$323 = 5 \cdot 64 + 3 = 5 \cdot (2 \cdot 5^2 + 2 \cdot 5 + 4) + 3 = 2 \cdot 5^3 + 2 \cdot 5^2 + 4 \cdot 5 + 3$;

e, então, $323 = (2243)_5$. Dizemos que fizemos a *conversão* do 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: $z = (c_n c_{n-1} \ldots c_1 c_0)_b$, $c_0 = r(z, b)$, $c_1 = r(q(z, b), b)$ e, assim, sucessivamente.

Por exemplo, para se converter 45 para o sistema binário, temos

$45 = 2 \cdot 22 + 1$,
$22 = 2 \cdot 11 + 0$,
$11 = 2 \cdot 5 + 1$,
$5 = 2 \cdot 2 + 1$,
$2 = 2 \cdot 1 + 0$,
$1 = 2 \cdot 0 + 1$,

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 $(23501)_7 = 2 \cdot 7^4 + 3 \cdot 7^3 + 5 \cdot 7^2 + 0 \cdot 7 + 1$, temos 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 esta soma também é menor que a base, é feita utilizando a comutatividade e associatividade da soma.

Por exemplo, $3 + 5 = 5 + 3 = 5 + (2 + 1) = (5 + 2) + 1 = ((5 + (1 + 1)) + 1 = ((5 + 1) + 1) + + 1 = (6 + 1) + 1 = 7 + 1 = 8$ e $(4)_7 + (2)_7 = (4)_7 + (1 + 1)_7 = (4 + 1)_7 + (1)_7 = (5)_7 + (1)_7 = (6)_7$.

(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 nos sistema decimal.

(iii) A soma de inteiros positivos y e z, menores que a base, quando esta 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 $x = (c_n c_{n-1} \ldots c_1 c_0)_b$ e $y = (d_m d_{m-1} \ldots d_1 d_0)_b$, temos $x = c_n \,.\, b^n + c_{n-1} \,.\, b^{n-1} + \ldots + c_1 \,.\, b + c_0$ e $y = d_m \,.\, b^m + d_{m-1} \,.\, b^{m-1} + \ldots + d_1 \,.\, b + d_0$ e então, se $n > m$,

$$x + y = c_n \,.\, b^n + c_{n-1} \,.\, b^{n-1} + \ldots + (c_m + d_m) \,.\, b^m + (c_{m-1} + d_{m-1}) \,.\, b^{m-1} + \ldots + (c_1 + d_1).\, b + (c_0 + d_0).$$

Se $c_i + d_i < b$, não há problema. Agora, $c_i + d_i \geq b$, 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 $x = (c_n c_{n-1} \ldots c_1 c_0)_b$ e $y = (d_m d_{m-1} \ldots d_1 d_0)_b$:

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

$$\begin{array}{r} 32767 \\ \underline{\ 9182} \\ 41949 \end{array}$$

Para somar $x = (3014)_6$ com $y = (5323)_6$, temos

$$\begin{array}{r} 3014 \\ \underline{5323} \\ 12341 \end{array}$$

Evidentemente, por associatividade, este 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, $x = (c_n c_{n-1}...c_1 c_0)_b$ e $y = (d_m d_{m-1}...d_1 d_0)_b$, escrevemos suas expressões b-ádicas $x = c_n . b^n + c_{n-1} . b^{n-1} + ... + c_1 . b + c_0$ e $y = d_m . b^m + d_{m-1} . b^{m-1} + ... + d_1 . b + d_0$ e aplicamos a distributividade da multiplicação em relação à soma

$$x . y = (c_n . b^n + c_{n-1} . b^{n-1} + ... + c_1 . b + c_0) . (d_m . b^m + d_{m-1} . b^{m-1} + ... + d_1 . b + d_0),$$

$$x . y = ((d_0 . c_n) . b^n + (d_o . c_{n-1}) . b^{n-1} + ... + (d_0 . c_1) . b + (d_0 . c_0)) + ((d_1 . c_n) . b^{n+1} + (d_1 . c_{n-1}) . b^n + ... + (d_1 . c_1) . b^2 + (d_1 . c_0) . b) + ... + ((d_m . c_n) . b^{m+n} + (d_m . c_{n-1}) . b^{m+n-1} + ... + (d_m . c_1). b^{m+1} + (d_m . c_0) . b^m).$$

Por exemplo,

$483 . 34 = (4 . 10^2 + 8 . 10 + 3) . (3 . 10 + 4),$
$483 . 34 = ((4 . 4) . 10^2 + (4 . 8) . 10 + (4 . 3)) + ((3 . 4) . 10^3) + (3 . 8) . 10^2 + (3 . 3) . 10),$
$483 . 34 = 12 . 10^3 + (16 + 24) . 10^2 + (32 + 9) . 10 + 12,$
$483 . 34 = 12 . 10^3 + 40 . 10^2 + 41 . 10 + 12,$
$483 . 34 = (10^4 + 2 . 10^3) + (4 . 10^3) + (4 . 10^2 + 1 . 10) + (10 + 2),$
$483 . 34 = 1 . 10^4 + 6 . 10^3 + 4 . 10^2 + 2 . 10 + 2,$
$483 . 34 = 16.422,$

onde da quarta para a quinta igualdades usamos as igualdades

$12 . 10^3 = (10 + 2) . 10^3 = 10^4 + 2 . 10^3,$
$40 . 10^2 = (4 . 10) . 10^2 = 4 . 10^3,$
$41 . 10 = (40 + 1) . 10 = 4 . 10^2 + 1 . 10.$

5.6 Aplicações à computação

5.6.1 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, estas 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 destes 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 esta 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*). Neste 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 que 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, esta função será representada por Ascii(x).

Uma questão a ser levantada: sendo o código Ascii(Z) = 90, por que Ascii(a) = 97 e não Ascii(a) = 91, como uma "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. Isto 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.

5.6.2 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 deste 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 $z = 2^{n-1} + 2^{n-2} + ... + 2 + 1$. Como, pelo exercício 3.17,

$$a^n - b^n = (a - b) \cdot (a^{n-1} + a^{n-2} \cdot b + a^{n-3} \cdot b^2 + \ldots + a \cdot b^{n-2} + b^{n-1}),$$

quaisquer que sejam os inteiros a, b e n, com $n > 1$, temos, para $a = 2$ e $b = 1$,

$$2^n - 1^n = (2 - 1) \cdot (2^{n-1} + 2^{n-2} + ... + 2 + 1)$$

e, assim, $z = 2^n - 1$.

As formas de armazenamento de um inteiro negativo fogem ao escopo deste livro.

5.6.3 Divisão por dois em computadores

Seja um inteiro b, maior que 1, e seja um inteiro positivo z, cuja representação no sistema de base b é $z = (c_n c_{n-1}...c_1 c_0)_b$. Desta forma temos $z = c_n \cdot b^n + c_{n-1} \cdot b^{n-1} + ... + c_1 \cdot b + c_0$ o que implica $z = (c_n \cdot b^{n-1} + c_{n-1} \cdot b^{n-2} + ... + c_1) \cdot b + c_0$. Assim, 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 num 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.

5.6.4 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

$$z^n = \begin{cases} 1, se\ n = 0 \\ z \cdot z^{n-1}, se\ n > 0 \end{cases}$$

No exercício referido se pedia para provar que

a) $a^m \cdot a^n = a^{m+n}$.
b) $(a^m)^n = a^{m \cdot n}$.
c) $a^m \cdot b^m = (a \cdot b)^m$.

Estas propriedades permitem que se estabeleça facilmente um algoritmo para calcular um potência z^n, dados z e n, como vimos no capítulo 4.

Algoritmo potencia
    leia(z, n);
    $p := 1$;
    $i := 1$;
    repita enquanto $n \geq i$
        $p := p \cdot z$;

$i := i + 1;$
escreva(p);

Por exemplo, a tabela abaixo mostra a execução deste 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.

A representação do expoente no sistema binário e as propriedades acima podem ser utilizadas para se obter um algoritmo como um número de iterações sensivelmente menor.

Para se calcular x^5, podemos pensar em

$$x^5 = x^{1.2^2+1} = \left(x^2\right)^2 . x^1 ,$$

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 $i = 0, 1, ..., s$, teremos

$$z^n = (z^2)^{a_s . 2^{s-1} + ... + a_2 . 2 + a_1} . z^{a_0}.$$

Fazendo $p_1 = z^{a_0}$, teremos

$$z^n = (z^2)^{a_s . 2^{s-1} + ... + a_2 . 2 + a_1} . p_1$$

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 $r(n, 2) = 0$.

Da igualdade acima, temos

$$z^n = (z^4)^{a_s . 2^{s-2} + ... + a_2} . (z^2)^{a_1} . p_1$$

e, fazendo $p_2 = \left(z^2\right)^{a_1} . p_1$, obtemos

$$z^n = (z^8)^{a_s . 2^{s-3} + ... + a_3} . (z^4)^{a_2} . p_2$$

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* se encontram no exercício 5.7).

Para $z = 3$ e $n = 13$, por exemplo, teríamos, $3^{13} = 3^{1.2^3+1.2^2+0.2^1+1} = \left(3^2\right)^{1.2^2+1.2+0.1} . 3^1$ e, então, $p_1 = 3$.

Continuando, $3^{13} = \left(\left(3^2\right)^2\right)^{1.2^1+1.1} . \left(3^2\right)^0 . p_1$; $p_2 = 1 . p_1 = 3$ e $3^{13} = \left(\left(3^4\right)^2\right)^{1.1} . \left(\left(3^2\right)^2\right)^1 . p_2$ o que dá $p_3 = \left(3^2\right)^2 . p_2 = 9^2 . 3 = 243$. Finalmente, $p_4 = \left((3)^4\right)^2 . 243$.

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.

5.7 Exercícios

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. Seja um inteiro z tal que $r(z, 4) = 3$. Prove que $r(z^2, 8) = 1$.

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 $(a_1, a_2, a_3, \ldots, a_{348})$ de inteiros contém as quantidades mensais de automóveis produzidos no Brasil no período de janeiro de 1980 a dezembro de 2008, qual o mês e o ano que correspondem à componente de ordem k..

5.7. Pela divisão euclidiana todo inteiro é da forma $2 \cdot n$ ou da forma $2 \cdot n + 1$, para algum inteiro n. Os inteiros da forma $2 \cdot n$ são chamados *pares* e os da forma $2 \cdot n + 1$ são chamados *ímpares*. Mostre que

a) A soma de dois inteiros pares é par.

b) A soma 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.

5.8. Mostre que $z^n + z$ 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 pelo menos um deles é par.

5.10. Mostre que todo inteiro z se escreve de modo único como $z = 3 \cdot q + s$, com q inteiro e $s \in \{-1, 0, 1\}$.

5.11. Mostre que a diferença de quadrados de dois ímpares é múltiplo de 8.

5.12. Considere os inteiros positivos m, n e a, com $m > n > 1$. Determine as cardinalidades dos

conjuntos

a) $\{z \in \mathbb{Z} \mid 0 < z \leq m \text{ e } a|z\}$.

b) $\{z \in \mathbb{Z} \mid n < z < m \text{ e } a|z\}$.

5.13. Mostre que são iguais os algarismos da casa das unidades de n^5 e n, qualquer que seja o inteiro positivo n.

5.14 Mostre que se a e b são inteiros

a) e n é um inteiro positivo, então $(a - b)|(a^n - b^n)$.

b) e n é um inteiro positivo ímpar, então $(a + b)|(a^n + b^n)$.

c) e n é um inteiro positivo par, então $(a + b)|(a^n - b^n)$.

5.15. Mostre que se k é um inteiro positivo par, então $3|(2^k - 1)$.

5.16. 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 $2^r - 1$.

5.17. Sejam $n, p \in \mathbb{Z}$, com $p < n$. Prove que

a) $p!$ divide $n . (n - 1) . (n - 2) . \ldots . (n - p + 1)$.

b) $p! . (n - p)!$ divide $n!$.

Considerando o item b acima, definimos *número binomial n sobre p* por $C_{n,p} = \dfrac{n!}{p!.(n-p)!}$

Vale observar que o *número binomial n sobre p* pode também ser representado por $\binom{n}{p}$

5.18. Mostre que $C_{n,p} + C_{n,p+1} = C_{n+1,p+1}$, expressão conhecida como *relação de* Stifel.

5.19. Mostre que, dados $a, b, n \in \mathbb{Z}$, com $n \geq 1$, temos

$$(a + b)^n = a^n + C_{n,1} . a^{n-1} . b + \ldots + C_{n,i} . a^{n-i} . b^i + \ldots + b^n,$$

fórmula conhecida como *Binômio de Newton*.

5.20. Mostre que, para todo inteiro positivo n, $C_{n,0} + C_{n,1} + C_{n,2} + \ldots + C_{n,n} = 2^n$.

5.21. Seja $a = (a_n a_{n-1} \ldots a_1 a_0)_{10}$. 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 $4|(a_1 a_0)_{10}$.

5.22. Utilizando a simbologia $\underline{ab}$ 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 $\underline{(a5)}^2 = \underline{a.(a+1)}25$ (isto significa que o quadrado de 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 pelo seu consecutivo: $35^2 = 1225$, pois $3 . 4 = 12$).

5.23. Mostre que se $4|k$,então o algarismo da casa das unidades de 2^k é igual a 6.

5.24. Mostre que todo inteiro da forma 44...488...89, com a quantidade de dígitos 8 sendo o antecessor da quantidade de dígitos 4, é um quadrado perfeito.

5.25. Determine em que base o número 54 do sistema decimal é representado por $(105)_b$.

5.26. Mostre que não existe base na qual o número decimal 24 é representado por $(108)_b$.

5.27. 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

5.28. Encontre um critério para verificar se um dado número representado no sistema de base b é par.

5.29. Considerando o exercício 5.9, 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 $(52)_{10}$ para o sistema de base 3'.

5.30. 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 $(1 + 3 + 3^2 + \ldots + 3^{n-1})$ g.

6. 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: y é *divisor* de z (simbologia $y|z$) se existe q tal que $z = y \cdot q$. Nesta seção, procuraremos analisar os divisores comuns de dois inteiros dados, em particular, o *maior destes 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 que mdc(20, 24) = 4.

Observe que este 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 este 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 $mdc(z, y) = mdc(y, z - y \cdot m)$, qualquer que seja o inteiro m.

Demonstração

Sejam $d_1 = mdc(z, y)$ e $d_2 = mdc(y, z - y \cdot m)$. Vamos mostrar que $d_2 \leq d_1$ e que $d_1 \leq d_2$. De $d_2 = mdc(y, z - y \cdot m)$ temos que $d_2|y$ e $d_2|(z - y \cdot m)$. Daí, $d_2|z$. Assim, d_2 é divisor comum de z e y e então $d_2 \leq d_1$, já que $d_1 = mdc(z, y)$.

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 $z - y \cdot m = r$, 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 $mdc(z, y) = mdc(y, r)$.

Com a utilização deste corolário, a determinação de mdc(20, 24) seria:

$$mdc(20, 24) = mdc(24, 20) = mdc(20, 4) = mdc(4, 0) = 4,$$

sendo esta 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 às seguintes propriedades que decorrem imediatamente da definição e cujas demonstrações serão

deixadas como exercício.

Propriedades do máximo divisor comum

a) $mdc(a, b) = mdc(|a|, |b|)$.
b) $mdc(a, b) = mdc(b, a)$.
c) Se $b|a$, então $mdc(a, b) = |b|$.

Por exemplo, mdc(504, 540) = mdc(540, 504) = mdc(504, 36) = 36, pois 36|504.
Outro exemplo: 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

$z = y \cdot q_1 + r_1$, com $0 \le r_1 < y$
$y = r_1 \cdot q_2 + r_2$, com $0 \le r_2 < r_1$
$r_1 = r_2 \cdot q_3 + r_3$, com $0 \le r_3 < r_2$
$r_2 = r_3 \cdot q_4 + r_4$, com $0 \le r_4 < r_3$
. . .
$r_{n-4} = r_{n-3} \cdot q_{n-2} + r_{n-2}$, com $0 \le r_{n-2} < r_{n-3}$
$r_{n-3} = r_{n-2} \cdot q_{n-1} + r_{n-1}$, com $0 \le r_{n-1} < r_{n-2}$
$r_{n-2} = r_{n-1} \cdot q_n + r_n$, com $0 \le r_n < r_{n-1}$
. . .,

então existe n tal que $r_n = 0$ e $r_{n-1} = mdc(z, y)$.
Além disso, existem inteiros t e u tais que $t \cdot z + u \cdot y = mdc(z, y)$.

Demonstração

Das desigualdades relativas aos restos, temos que $y > r_1 > r_2 > r_3 > ... > r_n > ... \ge 0$ 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, de mdc(z, y) = r_{n-1} segue mdc(z, y) = r_{n-3} - r_{n-2} . q_{n-1}, na qual podemos substituir $r_{n-2} = r_{n-4} - r_{n-3} \cdot q_{n-2}$, obtendo mdc(z, y) = r_{n-3} - (r_{n-4} - r_{n-3} . q_{n-2}). q_{n-1}. Nesta igualdade podemos substituir $r_{n-3} = r_{n-5} - r_{n-4} \cdot q_{n-3}$, e, seguindo substituindo retroativamente, encontraremos t e u tais que $t \cdot z + u \cdot y = mdc(z , y)$.

A aplicação deste algoritmo "na mão" (isto é, com lápis e papel) pode ser feita no esquema abaixo, onde calculamos mdc(396, 84):

396	84	60	24	12	0
	4	1	2	2	

concluindo que $mdc(396, 84) = 12$.
Observe que este esquema é simplesmente uma maneira prática de se realizar as divisões

396 = 84 . 4 + 60,
84 = 60 . 1 + 24,
60 = 24 . 2 + 12,
24 = 12 .2 e $r_4 = 0$.

Para encontrar os inteiros m e n tais que $m \cdot 396 + n \cdot 84 = 12$ temos as seguintes igualdades:

12 = 60 – 2 . 24,
12 = 60 – 2 . (84 – 1 . 60) = -2 . 84 + 3 . 60,
12 = -2 . 84 + 3 . (396 - 84 . 4) = 3 . 396 – 14 . 84,

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 inteiros t e u tais $t \cdot z + u \cdot y = d$ não se tem necessariamente $d = \text{mdc}(z, y)$. 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 esta 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 deste algoritmo, que é medida pelo números 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 $t \cdot z + u \cdot y = mdc(z, y)$) na linguagem algorítmica foge ao escopo do livro.

6.3 Inteiros primos entre si

Na seção anterior afirmamos que a recíproca da segunda parte do Algoritmo de Euclides (se $d = \text{mdc}(z, y)$, então existem inteiros t e u tais que $t \cdot z + u \cdot y = d$) só era verdadeira se $d = 1$. Ou seja, como veremos na proposição seguinte, se existem inteiros t e u tais que $t \cdot z + u \cdot y = 1$, então $\text{mdc}(z, y) = 1$. Além da veracidade desta recíproca, o fato de o máximo divisor comum de dois inteiros ser igual a 1 é importante pois ele gera outras propriedades interessantes. Para facilitar a linguagem, quando mdc(z, y) = 1, dizemos que os dois inteiros z e y são *primos entre si* (ou *co-primos*) ou que um dos inteiros é *primo em relação ao outro*. Observe que desta 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 $z \cdot t + y \cdot u = 1$, então $mdc(z, y) = 1$.

Demonstração

Seja $d = \text{mdc}(z, y)$. Assim, $d|z$ e $d|y$ o que implica $d|(z \cdot t + y \cdot u)$. 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 $b|(a \cdot c)$, então $b|c$.
b) Se $a|c$ e $b|c$, então $(a \cdot b)|c$.

Demonstração

a) Como a e b são primos entre si, existem inteiros m e n tais que $a \,.\, m + n \,.\, b = 1$. Daí, multiplicando ambos os termos desta igualdade por c, temos $a \,.\, m \,.\, c + n \,.\, b \,.\, c = c$. Como b divide as duas parcelas, temos $b|c$.

b) Da hipótese de que $a|c$ temos que existe q_1 tal que $c = a \,.\, q_1$. Assim, da hipótese $b|c$, segue que $b|(a \,.\, q_1)$. Então, pelo item (a), $b|q_1$ e, portanto, existe q_2 tal que $q_1 = b \,.\, q_2$. Substituindo isto em $c = a \,.\, q_1$, temos que $c = a \,.\, b \,.\, q_2$, o que mostra que $(a \,.\, b)|c$.

Observe que a hipótese de que 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 $a \,.\, x + b \,.\, y = c$, 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 $a \,.\, k + b \,.\, j = c$.

Por exemplo, (10, -7) é uma solução da equação diofantina $5 \,.\, x + 7 \,.\, y = 1$. Por sua vez, a equação $2 \,.\, x + 4 \,.\, y = 5$ não tem solução: qualquer que seja o par de inteiros (k, j), $2 \,.\, k + 4 \,.\, j$ 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 $d = \text{mdc}(a, b)$. A equação diofantina $a \,.\, x + b \,.\, y = c$ é solúvel se e somente se $d|c$.

Demonstração

Suponhamos que (k, j) seja uma solução da equação $a \,.\, x + b \,.\, y = c$. Assim, $a \,.\, k + b \,.\, j = c$. Daí, como $d|a$ e $d|b$, segue que $d|c$.

Reciprocamente, suponhamos que exista um inteiro t tal que $c = d \,.\, t$. Do algoritmo de Euclides temos que existem inteiros m e n tais que $a \,.\, m + b \,.\, n = d$ e, portanto, $a \,.\, m \,.\, t + b \,.\, n \,.\, t = d \,.\, t$. Assim, o par $(m \,.\, t \,,\, n \,.\, t)$ é solução da equação $a \,.\, x + b \,.\, y = c$.

Por exemplo, para encontrar uma solução da equação $361 \,.\, x + 160 \,.\, y = 3$, temos

361	160	41	37	4	1
	2	3	1	9	

e, então, $1 = 37 - 9 \,.\, 4 = 37 - 9 \,.\, (41 - 37 \,.\, 1) = -9 \,.\, 41 + 10 \,.\, 37 = -9 \,.\, 41 + 10 \,.\, (160 - 41 \,.\, 3) = 10 \,.\, 160 - 39 \,.\, 41 = 10 \,.\, 160 - 39 \,.\, (361 - 160 \,.\, 2) = -39 \,.\, 361 + 88 \,.\, 160$. Portanto uma solução da equação é $(-39 \,.\, 3,\ 88 \,.\, 3) = (-117, 264)$.

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 $a \,.\, x + b \,.\, y = c$, então, qualquer que seja o inteiro k, o par $\left(t - k \,.\, \frac{b}{d}, u + k \,.\, \frac{a}{d}\right)$ também o é.

6.5 Números primos

Veremos agora os inteiros especiais citados na introdução deste capítulo. Veremos que há números que são os "átomos" dos conjuntos 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 que 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 alguns autores usam-na para definir número primo. Para estes autores, a definição acima é estudada como uma propriedade.

Proposição 4.6

Sejam p um número primo e a e b inteiros positivos. Se $p|(a \,.\, b)$, então $p|a$ ou $p|b$.

Demonstração

Suponhamos que p não divide a. Então, como p é primo, a e p são primos entre si. Da hipótese de que p|(a . b) segue (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. Isto 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. Suponhamos que d não seja primo. Então existe 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 este algoritmo para a entrada $z = 847$, temos a saída $d = 7$, pois $847 = 7 \,.\, 121$, 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 acima quando a entrada é um número primo p, exige p laços. Na verdade isto 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 $z = d \,.\, q$. 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 $d^2 \leq z$.

Esta 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 acima 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 esta melhora o algoritmo fica muito ineficiente se z é um número primo muito grande. Observe que em cada laço são efetuadas um 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 - esta 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. Este 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 ações solicitadas apresentadas no quadro a seguir.

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 destes números.

5. Como $47^2 > 300$, todos os números do crivo não riscados são primos.

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 neste 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. Este 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, $i! \cdot (p - i)!$. $C_{p,i} = p!$ 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 isto, 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

$$(a + 1)^p - (a + 1) = (a^p + C_{p,1} \cdot a^{p-1} + ... + C_{p,,i} \cdot a^{p-i} + ... + C_{p,p-1} \cdot a + 1) - (a + 1) =$$
$$= (a^p - a) + (C_{p,1} \cdot a^{p-1} + ... + C_{p,,i} \cdot a^{p-i} + ... + C_{p,p-1} \cdot a),$$

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 um inteiro 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 positivo tal que $k > 1$ 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, os cientistas indianos Manindra Agrawal, Neeraj Kayal e Nitin Saxena encontraram uma solução para esta questão (Coutinho, S. C. - 2004).

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 $z = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_k^{e_k}$, 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 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, …, 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

$$q_i = q_{i+1} = \ldots = q_{i+e_i}, q_i . q_{i+1} \ldots . q_{i+e_i} = p_i^{e_i} \text{ , com } p_i = q_i.$$

Para provar a unicidade, seja S o conjunto dos inteiros positivos que podem ser fatorados de duas maneiras distintas e suponhamos que $S \neq \varnothing$.

Como S é limitado inferiormente, pelo Princípio da Boa Ordenação, S tem um elemento mínimo n. Assim, $n = p_1^{e_1} . p_2^{e_2} \ldots . p_k^{e_k} = q_1^{f_1} . q_2^{f_2} \ldots . q_l^{f_l}$, onde os primos da fatoração do primeiro membro são distintos dos primos da fatoração do segundo membro ou, se os primos das duas fatorações são iguais, os expoentes correspondentes são diferentes. Ora, como $p_1 | n$, temos que $p_1 | (q_1^{f_1} . q_2^{f_2} \ldots . q_l^{f_l})$ 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 $n = p_1^{e_1} . p_2^{e_2} \ldots . p_k^{e_k} = q_1^{f_1} . q_2^{f_2} \ldots . p_1^{l_j} \ldots . q_l^{f_l}$.

Aplicando a lei da cancelamento à igualdade acima, dividindo-a por p_1, obtemos

$$m = p_1^{e_1 - 1} . p_2^{e_2} \ldots . p_k^{e_k} = q_1^{f_1} . q_2^{f_2} \ldots . p_1^{l_j - 1} . q_l^{f_l}$$

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 $5.292 = 2^2 \cdot 3^3 \cdot 7^2$.

A expressão $z = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_k^{e_k}$ gerada pelo algoritmo acima 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 $p\# = p \cdot q\#$, onde q é o maior primo menor que p, se $p > 2$. Por exemplo, $3\# = 3 \cdot 2\# = 3 \cdot 2 = 6$ e $5\# = 5 \cdot 3\# = 5 \cdot 6 = 30$. Observe que esta definição diz trivialmente que, para $p > 2$, $p\#$ é o produto de todos os primos positivos menores 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.

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, para todo inteiro n, os n inteiros $(n + 1)! + 2$, $(n + 1)! + 3$, ..., $(n + 1)! + (n + 1)$ são números compostos, pois $2|((n + 1)! + 2)$, $3|((n + 1)! + 3)$, ..., $(n+1)|((n + 1)! + (n + 1))$.

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 haja a conjectura que este número seja infinito. Em dezembro de 2011 foi encontrado um par de primos gêmeos com 200 700 dígitos (http://primes.utm.edu/top20/page.php?id=1, acessada em 28/11/2013).

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 seguinte 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**, que possui 169.966 dígitos (http://primes.utm.edu/top20/page.php?id=5, acessada em 16/11/2011).

Uma outra fórmula tentada foi a *fórmula polinomial* que foi descartada em função de um teorema cuja demonstração de um caso particular é solicitada no exercício 6.15 abaixo.

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 destas 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 $\left(2^{n_1}\right)^{n_2} - 1 = 2^n - 1$, temos $\left(2^{n_1} - 1\right)|\left(2^n - 1\right)$ 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 deste 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 desta forma ou que, pelo menos, esta 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 21/07/2011) cujo objetivo é encontrar primos de Mersenne.

Em 23 de agosto de 2008, foi encontrado o 45° primo de Mersenne conhecido: $2^{43.112.609} - 1$, com 12.978.189 dígitos, feito que foi contemplado com um prêmio de cem mil dólares, dado pela

Electronic Frontier Foundation, uma fundação norte-americana. Em 12 de abril de 2009, foi encontrado o 47º conhecido: $2^{42.643.801} - 1$, com 12.837.04 dígitos.

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 $z = 2^m \cdot r$, com m inteiro positivo e r ímpar e então, do exercício 5.12, $\left(z^{2^m}+1\right) \mid \left(\left(z^{2^m}\right)^r+1\right)$. Como $\left(z^{2^m}\right)^r+1 = z^n+1$ 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*, devido ao fato de que 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 21/07/2011) 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) da Teoria dos Números. Em 7 de julho de 1742, Christian Goldbach, matemático prussiano, numa carta que escreveu ao matemático suíço Leonard Euler fez a seguinte observação: *qualquer número ímpar maior que cinco parecia 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 07/06/2013).

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 $4 \cdot 10^{18}$ (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 a ser 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). Num instante de genialidade, Fermat percebeu que não existiriam inteiros distintos x, y e z tais que $x^3 + y^3 = z^3$. Evidentemente, esta 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 esta proposição mas esta margem é muito estreita para contê-la.*

Nos últimos 350 anos, muitos matemáticos famosos tentaram demonstrar o teorema de Fermat, o que só foi conseguido por Andrew Wiles em 1995. Este 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

6.1. Mostre que, qualquer que seja o inteiro n maior que 1, os pares de inteiros abaixo são primos entre si.

a) $2 \cdot n + 1$ e $3 \cdot n + 1$.
b) $2 \cdot n + 1$ e $6 \cdot n + 1$.
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 $361 \cdot t + 160 \cdot u = 1$.

6.3. Por uma generalização muito razoável, o máximo divisor comum de vários números é o *maior* inteiro que é divisor dos números. Mostre que, se a_1, a_2, ..., a_n são inteiros, então $mdc(a_1, a_2, ..., a_n) = mdc(mdc(a_1, a_2), a_3, ..., a_n)$.

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 $mdc(a \cdot b, c) = mdc(b, c)$.

6.6. Sejam a e b inteiros. 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 (simbologia: *mmc(z, y)*) é o *menor* inteiro que é múltiplo de z e múltiplo de y.

a) Mostre que $mmc(z, y) = \dfrac{z \,.\, y}{mdc(z,\ y)}$

b) Mostre que se a é um inteiro tal que $z|a$ e $y|a$, então $mmc(z, y)|a$.

6.10. Sejam a e b dois inteiros. Mostre que se a e b forem positivos então o conjunto das soluções positivas da equação $a \,.\, x + b \,.\, y = c$ é finito.

6.11. 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 maiores que 1. Mostre que $mdc(a^m - 1, a^n - 1) = a^d - 1$, onde $d = mdc(m, n)$.

6.13. Considerando que $n! = 1 \,.\, 2 \,.\, 3 \,.\, \ldots \,.\, (n\text{-}1) \,.\, n$, 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 $p + 2$. Na referida 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 chamada *funções polinômios*). Esta tentativa esbarrou no fato de que se pode provar que dado um polinômio $f(x)$ como acima, 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) $F_n = F_0 \,.\, F_1 \,.\, F_2 \,.\, \ldots \,.\, F_{n-1} + 2$.

c) Mostre que, se $m < n$, então $mdc(F_n, F_m) = 1$.

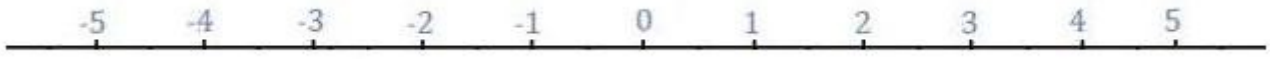
d) Use o resultado do item c para apresentar uma outra demonstração de que existem infinitos números primos.

6.17. Mostre que existe uma infinidade de trios pitagóricos (para quem não leu a seção 6.7, um *trio pitagórico* é um conjunto de números inteiros $\{x, y, z\}$ tal que $x^2 + y^2 = z^2$).

7. Os inteiros módulo n

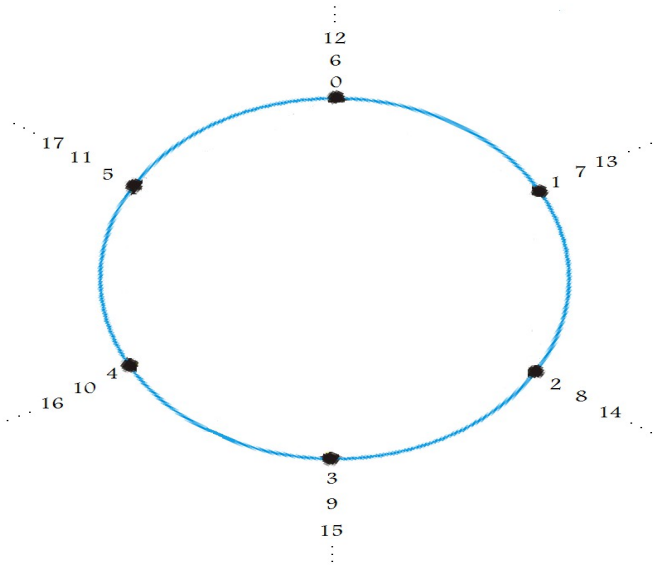
7.1 Introdução

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: (1) os pontos da forma $p_{2.k+1}$ estão situados à direita de p_0, com $p_{2.(k+1)+1}$ à direita de $p_{2.k+1}$ ($k = 0, 1, 2, ...$); (2) os pontos da forma $p_{2.k}$ estão situados à esquerda de p_0, com $p_{2.(k+1)}$ à esquerda de $p_{2.k}$ ($k = 0, 1, 2, ...$); (3) a distância entre dois pontos consecutivos é constante (*distância*, grandeza primitiva da Física) e definamos uma 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 abaixo, chamada *reta dos inteiros*.



Neste capítulo, vamos mostrar como a partir dos inteiros e de um inteiro $n > 1$ dado obter um novo anel. Estes anéis serão indicados por $\mathbb{Z}_n$, são chamados, para cada n, *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, objetivo final do capítulo.

"Geometricamente" falando, os anéis $\mathbb{Z}_n$ são obtidos transformando a reta dos inteiros numa circunferência, como mostra a figura abaixo 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 maior que 1 e definamos em $\mathbb{Z}$ a relação *congruência módulo n* por $a \equiv b \bmod n$ *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 que $r(7, 2) = 1$ (a simbologia $a \not\equiv b \ mod\ n$ indica, naturalmente, que a e b não são congruentes módulo n).

Vale observar que num 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 $a = n \,.\, q_1 + r$ e $b = n \,.\, q_2 + r$. 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 $a = n \,.\, q_1 + r_1$, com $0 \le r_1 < n$ e $b = n \,.\, q_2 + r_2$, com $0 \le r_2 < n$.

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 $|r_1 - r_2| < n$. Assim, $r_1 = r_2$ e $a \equiv b \ mod\ n$.

Uma consequência imediata desta proposição relaciona a congruência módulo n com a divisão euclidiana com divisor n.

Corolário 1.7

Sejam a e r inteiros, com $0 \le r < n$. 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 $a - r = n \,.\, q$. Assim, $a = n \,.\, q + r$ e, como $0 \le r < n$, temos $r = r(a, n)$.

Reciprocamente, se $r = r(a, n)$, existe um inteiro q tal que $a = n \,.\, q$ + r e, então, $a - r = n \,.\, q$ 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 $r(a, n) = a \ mod\ n$. Também poderemos escrever $a \ mod\ n = b \ mod\ n$ no lugar de $a \equiv b \ mod\ n$.

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 numa 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 $n|(a - c)$. Isto mostra que $a \equiv c \ mod \ n$.

Além de gozar das propriedades acima, a congruência goza de propriedades que podem ser relacionadas com a compatibilidade com as operações no conjunto dos inteiros, conforme mostra a seguinte proposição.

Proposição 3.7

Sejam a, b, c e d inteiros quaisquer.

a) Se $a \equiv b \ mod \ n$ e $c \equiv d \ mod \ n$, então $(a + c) \equiv (b + d) \ mod \ n$.
b) Se $a \equiv b \ mod \ n$ e $c \equiv d \ mod \ n$, então $(a \ . \ c) \equiv (b \ . \ d) \ mod \ n$.
c) Se m é um inteiro positivo e $a \equiv b \ mod \ n$, então $a^m \equiv b^m \ mod \ n$.

Demonstração

a) De $a \equiv b \ mod \ n$ e $c \equiv d \ mod \ n$ segue que $n|(a - b)$ 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 que $n|(a - b)$ e $n|(c - d)$. Daí, $n|(d \ . \ (a - b) + a \ . \ (c - d))$ o que implica $a \ . \ c \equiv b \ . \ d \ mod \ n$.
c) Provemos esta 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 isto 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 que $a \equiv r_1 \ mod \ n$ 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 $(a \,.\, c) \equiv (b \,.\, c)$ *mod* n e $mdc(c, n) = 1$, então $a \equiv b$ *mod* n.

c) Se $(a \,.\, b) \equiv (c \,.\, d)$ *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 $(a \,.\, c) \equiv (b \,.\, c)$ *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) Das duas primeiras hipóteses segue que existem inteiros i e j tais que $a \,.\, b - c \,.\, d = i \,.\, n$ e $a - c = j \,.\, n$. Substituindo $c = a - j \,.\, n$ na primeira destas equações obtemos $a \,.\, b - a \,.\, d + j \,.\, n \,.\, d = i \,.\, n$ o que implica $a \,.\, (b - d) = (i - j \,.\, d) \,.\, n$.

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 que a assertiva do item (c) uma generalização afirmação do item (b).

7.3 Uma aplicação: critérios de divisibilidade

Sabemos desde nossos estudos do ensino fundamental 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 este e outros critérios de divisibilidade.

Seja um inteiro z representado no sistema decimal por $z = a_n a_{n-1} \ldots a_2 a_1 a_0$. Assim, $z = a_n \,.\, 10^n + a_{n-1} \,.\, 10^{n-1} + \ldots + a_2 \,.\, 10^2 + a_1 \,.\, 10 + a_0$. 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 proposição citada, $a_i \,.\, 10^i \equiv a_i$ *mod* 9, para todo $i = 0, 1, \ldots, n$. Assim, somando estas congruências,

$$(a_n \,.\, 10^n + a_{n-1} \,.\, 10^{n-1} + \ldots + a_1 \,.\, 10 + a_0) \equiv (a_n + a_{n-1} + \ldots + a_1 + a_0) \text{ mod } 9$$

e, portanto, pelo corolário 2.7, $9|z$ se e somente se $9|(a_n + a_{n-1} + \ldots + a_1 + a_0)$.

Observe que o raciocínio desenvolvido acima 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

$$(a_n \,.\, 10^n + a_{n-1} \,.\, 10^{n-1} + \ldots + a_1 \,.\, 10 + a_0) \equiv (a_0 - a_1 + a_2 - a_3 + \ldots) \text{ mod } 11$$

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 $(a_n \,.\, 10^n + a_{n-1} \,.\, 10^{n-1} + \ldots + a_1 \,.\, 10 + a_0) \equiv (a_n + a_{n-1} + \ldots + a_1 + a_0)$ *mod* 9 mostrada acima e das propriedades das congruências módulo n segue que:

a) Se $z = a_n a_{n-1} \ldots a_2 a_1 a_0$, então $(z - (a_n + a_{n-1} + \ldots + a_1 + a_0)) \equiv 0$ *mod* 9 donde se conclui que $9|(z - (a_n + a_{n-1} + \ldots + a_1 + a_0))$.

b) Se $z = a_n a_{n-1} \ldots a_2 a_1 a_0$ e $y = b_n b_{n-1} \ldots b_2 b_1 b_0$ 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 estas 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 (idêntico àquele para o critério de divisibilidade por 3) concluímos que se $a_n a_{n-1}...a_1 a_0$ é a representação decimal de um inteiro z, então $r(z, 9) = r(a_n + a_{n-1} + ... + a_1 + a_0, 9)$ pois

$$(a_n . 10^n + a_{n-1} . 10^{n-1} + ... + a_1 . 10 + a_0) \equiv (a_n + a_{n-1} + ... + a_1 + a_0) \; mod \; 9.$$

O cálculo de $(a_n + a_{n-1} + ... + a_1 + a_0)$ *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, de acordo com o corolário 3.7, 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 dos fatos acima, temos que se $b = b_n b_{n-1}...b_1 b_0$, então novamente por aplicação $r(a . b, 9) = r((a_n + a_{n-1} + ... + a_1 + a_0) . (b_n + b_{n-1} + ... + b_1 + b_0), 9)$,

Estas igualdades podem ser utilizadas para se demonstrar um teste de verificação da correção de operações com inteiros, o conhecido teste da *prova dos nove*. Vamos mostrar o teste para a multiplicação. Sejam $a = a_n a_{n-1}...a_1 a_0$ e $b = b_n b_{n-1}...b_1 b_0$ dois inteiros representados no sistema decimal e $c = c_n c_{n-1}...c_1 c_0$ tal que $c = a . b$.

Pelos comentários acima, devemos ter, módulo 9,

$$(a_n + a_{n-1} + ... + a_1 + a_0) . (b_n + b_{n-1} + ... + b_1 + b_0) \equiv (c_n + c_{n-1} + ... + c_1 + c_0)$$

Utilizamos então o seguinte esquema

a'	b'
d'	c'

onde

$a' \equiv (a_n + a_{n-1} + ... + a_1 + a_0)\ mod\ 9$,
$b' \equiv (b_n + b_{n-1} + ... + b_1 + b_0)\ mod\ 9$,
$c' \equiv (c_n + c_{n-1} + ... + c_1 + c_0)\ mod\ 9$ e
$d' \equiv (a' . b')\ mod\ 9$.

Pelo acima exposto, 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 deste fato. Por exemplo, suponhamos que queiramos verificar a igualdade $425.638 \times 3.489 = 1.485.051.982$. Temos

$a' \equiv (4 + 2 + 5 + 6 + 3 + 8)\ mod\ 9 \equiv 1$,
$b' \equiv (3 + 4 + 8 + 9)\ mod\ 9 \equiv 6$,
$c' \equiv (1 + 4 + 8 + 5 + 0 + 5 + 1 + 9 + 8 + 2)\ mod\ 9 \equiv 7$,
$d' \equiv (a' . b')\ mod\ 9 \equiv (1 . 6)\ mod\ 9 \equiv 6$.

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.

$2^4 \equiv (-1)\ mod\ 17$,
$(2^4)^{35} \equiv (-1)^{35}\ mod\ 17$,
$2^{140} \equiv (-1)\ mod\ 17$,
$2^{143} = 2^{140} . 2^3 \equiv (-1) . 8\ mod\ 17 \equiv (-8)\ mod\ 17$.

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, $10^{45} \equiv 10^{6 . 7 + 3} \equiv (10^6)^7 . 10^3 \equiv 1 . 6 \equiv 6$ 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 na seção 5.5. Naturalmente, a única adaptação a fazer é efetuar as operações módulo n, obtendo então o seguinte algoritmo para calcular $z^e\ mod\ n$.

Algoritmo potência módulo n;
    leia(z, e, n);
    $b := z$; $m := e$; $p := 1$;

repita enquanto $m \neq 0$
  se resto(m, 2) $\neq 0$
    $p := b \,.\, p \; mod \; n$;
  $m :=$ quociente(m, 2);
  $b := (b \,.\, b) \; mod \; n$;
escreva(p);

A tabela a seguir apresenta a execução deste 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 $\overline{a} = \{x \in A | x \approx a\}$. 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), $a \in \overline{a}$ temos que $a \in \overline{b}$. Daí, $a \approx b$. Reciprocamente, suponhamos $a \approx b$ e tomemos $x \in \overline{a}$. Daí, $x \approx a$ e, por transitividade, $x \approx b$, o que implica $x \in \overline{b}$. Assim $\overline{a} \subset \overline{b}$. *Mutatis mutandis*, se mostra que $\overline{b} \subset \overline{a}$.

c) Se $\overline{a} \cap \overline{b} \neq \emptyset$, existe $x \in \overline{a}$ e $x \in \overline{b}$ o que implica que existe $x \in A$ tal que $x \approx a$ e $x \approx b$. Daí, por reflexividade e transitividade, $a \approx b$ e, então, pelo item (*b*), $\overline{a} = \overline{b}$. Porém, isto contraria a hipótese.

As classes de equivalência da relação *congruência módulo n* são chamadas *classes residuais módulo n* e qualquer inteiro b tal que $\overline{a} = \overline{b}$ é dito *um representante* da classe residual $\overline{a}$.

Por exemplo, existem duas classes residuais módulo 2:

$\overline{0} = \{\ldots -4, -2, 0, 2, 4 \ldots\}$
$\overline{1} = \{\ldots -3, -1, 1, 3, \ldots\}$

o que mostra que qualquer número par é representante da classe $\overline{0}$ e qualquer número ímpar é representante da classe $\overline{1}$.

De forma semelhante, existem três classes residuais módulo 3. A classe $\overline{0}$ que contém os múltiplos de 3, a classe $\overline{1}$ que tem como representantes os inteiros da forma $3 \,.\, q + 1$ e a classe $\overline{2}$ com representantes da forma $3 \,.\, q + 2$.

O fato de existirem duas classes residuais módulo 2 e três classes residuais módulo 3 não é privilégio destes dois inteiros como mostra a seguinte proposição.

Proposição 6.7

Existem exatamente n classes residuais módulo n: $\overline{0}, \overline{1}, \ldots, \overline{(n-1)}$.

Demonstração

Provemos inicialmente as n classes listadas acima 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 a inteiro, pela divisão euclidiana, existem inteiros q e r tais que $a = n \,.\, q + r$, 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 $\overline{0}, \overline{1}, \ldots, \overline{(n-1)}$.

O conjunto das classes residuais módulo n $\{ \overline{0}, \overline{1}, \ldots, \overline{(n-1)} \}$ é indicado por $\mathbb{Z}_n$ e é denominado *conjunto dos inteiros módulo n*. É habitual, num 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 os mesmos operadores + e . das operações em $\mathbb{Z}$, utilizadas nos segundos membros.

Adição: $\overline{a} + \overline{b} = \overline{a+b}$
Multiplicação: $\overline{a} \,.\, \overline{b} = \overline{a \,.\, b}$

Evidentemente, é necessário garantir que estas 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. Isto significa que devemos provar que se $x \in \overline{a}$ e $y \in \overline{b}$, então $\overline{x+y} = \overline{a+b}$ e $\overline{x \,.\, y} = \overline{a \,.\, b}$. Estas igualdades, porém, decorrem da proposição 3.7, pois $x \in \overline{a}$ e $y \in \overline{b}$ 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,

$$\overline{a} + \overline{b} = \overline{a+b} = \overline{b+a} = \overline{b} + \overline{a}$$

e

$$\overline{a} \,.\, (\overline{b} \,.\, \overline{c}) = \overline{a} \,.\, \overline{b \,.\, c} = \overline{a \,.\, (b \,.\, c)} = \overline{(a \,.\, b) \,.\, c} = \overline{a \,.\, b} \,.\, \overline{c} = (\overline{a} \,.\, \overline{b}) \,.\, \overline{c} \,.$$

O elemento neutro da adição é $\overline{0}$, pois $\overline{a} + \overline{0} = \overline{a+0} = \overline{a}$ e o elemento neutro da multiplicação é $\overline{1}$, pois $\overline{a} \,.\, \overline{1} = \overline{a \,.\, 1} = \overline{a}$. O simétrico de uma classe $\overline{a}$ é classe $\overline{n-a}$, pois

$\overline{a}+\overline{n-a}=\overline{a+(n-a)}=\overline{n}=\overline{0}$. A distributividade da multiplicação em relação à adição também é simples de provar e decorre da propriedade respectiva do anel dos inteiros:

$$\overline{a}\ .\ (\overline{b}+\overline{c})=\overline{a}\ .\ \overline{b+c}=\overline{a\ .\ (b+c)}=\overline{a\ .\ b+a\ .\ c}=\overline{a\ .\ b}+\overline{a\ .\ c}=\overline{a}\ .\ \overline{b}+\overline{a}\ .\ \overline{c}$$

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 que 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 $\overline{2}\ .\ \overline{2}=\overline{0}$, enquanto que $\mathbb{Z}_3$ o é. Observe também que em $\mathbb{Z}_4$ o inverso de $\overline{3}$ é o próprio $\overline{3}$ e que $\overline{2}$ não tem inverso: não existe a tal que $2\ .\ a = 1$.

É simples realizar operações em $\mathbb{Z}_n$ mesmo que n seja grande. Basta observar que, por exemplo, $\overline{a}\ .\ \overline{b}=\overline{r}$, onde $r = r(a\ .\ b, n)$. 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 $\overline{0}$. 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 $a\ .\ b \equiv 1\ mod\ n$. Assim, $n|(a\ .\ b - 1)$ e, daí, existe $t \in \mathbb{Z}$ tal que $a\ .\ b - 1 = n\ .\ t$. Concluímos então que existem inteiros b e t tais que $a\ .\ b + n\ .\ t = 1$ o que implica, pela proposição 1.6, que a e n são primos entre si.

Reciprocamente, se $mdc(a, n) = 1$, então existem inteiros b e t tais que $a\ .\ b + n\ .\ t = 1$. Daí, $a\ .\ b = n\ .\ t + 1$ o que implica $a\ .\ b \equiv 1\ mod\ n$. Logo, em $\mathbb{Z}_n$, $a\ .\ b = 1$ e a é inversível.

Como foi dito acima, a demonstração anterior 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

$a \,.\, b + n \,.\, t = 1$, 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

$1 = 11 - 5 \,.\, 2$
$1 = 11 - 5 \,.\, (13 - 1 \,.\, 11) = -5 \,.\, 13 + 6 \,.\, 11$
$1 = -5 \,.\, 13 + 6 \,.\, (50 - 3 \,.\, 13) = 6 \,.\, 50 - 23 \,.\, 13$
$1 = 6 \,.\, 50 - 23 \,.\, (63 - 1 \,.\, 50) = - 23 \,.\, 63 + 29 \,.\, 50$
$1 = -23 \,.\, 63 + 29 \,.\, (176 - 2 \,.\, 63) = 29 \,.\, 176 - 81 \,.\, 63.$

Daí, $b = -81$ e $63^{-1} = -81 = 176 - 81 = 95$. Observe que, de fato, $63 \,.\, 95 = 5.985 \equiv 1 \; mod \; 176$.

A determinação do inverso de 13 em $\mathbb{Z}_{40}$ seria bem mais simples: como

40	13	1
	3	

temos $1 = 40 - 13 \,.\, 3$ 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 $\overline{1}, \overline{2}, \ldots, \overline{p-1}$ 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 $m = i \,.\, p$ para algum $i = 1, 2, 3, \ldots, p^{n-1}$.

Demonstração

Seja $d = mdc(m, k)$. Se $m = i \,.\, p$ 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 $m = t \,.\, p^j$ para algum $1 < j < p$ e algum inteiro t. Dessa forma, $m = (t \,.\, p^{j-1}) \,.\, p$ 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 $(a \,.\, x) \equiv b \; mod \; n$. Um inteiro x_0 tal que $a \,.\, x_0 \equiv b \; mod \; n$ é dito uma *solução* da congruência. Por exemplo, $x_0 = 15$ é uma solução da congruência $3 \,.\, x \equiv 5 \; mod \; 8$, pois $45 \equiv 5 \; mod \; 8$.

Por transitividade, se x_0 é uma solução da congruência $a \,.\, x \equiv b \; mod \; n$ 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 $a \,.\, x \equiv b \; mod \; n$ é equivalente à equação $\overline{a} \,.\, \overline{x} = \overline{b}$. Assim, naturalmente, uma classe residual solução da equação $\overline{a} \,.\, \overline{x} = \overline{b}$ é dita também uma *solução módulo n* da congruência $(a \,.\, x) \equiv b \; mod \; n$.

É muito fácil ver que se a e n são primos entre si, então a congruência $a \,.\, x \equiv b \; mod \; n$ tem uma única solução módulo n. De fato, da hipótese de que a e n são primos entre si segue que $\overline{a}$ é inversível em $\mathbb{Z}_n$ e, assim, $x_0 = (\overline{a})^{-1} \,.\, \overline{b}$ é a solução única da congruência.

Por exemplo, como $(\overline{3})^{-1} = \overline{3}$, temos que $x_0 = (\overline{3})^{-1} \,.\, \overline{5} = \overline{3} \,.\, \overline{5} = \overline{7}$ é a única solução da congruência $3 \,.\, x \equiv 5 \; mod \; 8$.

Naturalmente, uma congruência do tipo $(a \,.\, x + c) \equiv b \; mod \; n$ também é uma congruência linear pois ela equivalente à congruência $(a \,.\, x) \equiv (b - c) \; mod \; n$. Por exemplo, $(5 \,.\, x + 9) \equiv 7 \; mod \; 6$ é equivalente a $(5 \,.\, x) \equiv (-2) \; mod \; 6 \equiv 4 \; mod \; 6$. Como em $\mathbb{Z}_6$, $(\overline{5})^{-1} = \overline{5}$, temos que $x \equiv (5 \,.\, 4) \; mod \; 6 \equiv 2 \; mod \; 6$, e, portanto, $\overline{2}$ 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 $a \,.\, x \equiv b \; mod \; n$ tem solução se e somente se $d|b$.

Demonstração

Suponhamos que exista um inteiro x_0 tal que $a \,.\, x_0 \equiv b \; mod \; n$. Então $n|(a \,.\, x_0 - b)$ e, portanto, existe um inteiro y_0 tal que $a \,.\, x_0 - b = n \,.\, y_0$. Daí, como $d|a$ e $d|n$, segue que $d|b$.

Reciprocamente, suponhamos que $d|b$. Assim, existe q tal que $b = d \,.\, q$. Por outro lado, como $d = mdc(a, n)$, existem inteiros x_0 e y_0 tais que $a \,.\, x_0 + n \,.\, y_0 = d$. Daí, $a \,.\, x_0 \,.\, q + n \,.\, y_0 \,.\, q = b$ e, portanto, $x_0 \,.\, q$ é uma solução da congruência $a \,.\, x \equiv b \; mod \; n$.

Por exemplo, consideremos a congruência $6 \,.\, x \equiv 4 \; mod \; 8$. 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, $2 = 8 - 6 \,.\, 1$. Portanto, $4 = 2 \,.\, 8 + 6 \,.\, (-2)$ o que mostra que $6 \,.\, (-2) \equiv 4 \; mod \; 8$. Daí, $x_0 = \overline{-2} = \overline{6}$ é uma solução da congruência. Da igualdade $2 = 8 - 6 \,.\, 1$, segue também que $2 + (-6) = 8 - 6 \,.\, 1 + (-6)$ o que dá $-4 = 8 - 6 \,.\, 2$. Esta última igualdade mostra que $6 \,.\, 2 \equiv 4 \; mod \; 8$ e, então, $\overline{2}$ é outra solução da congruência.

Observe que a demonstração acima foi baseada no fato óbvio de que a congruência $a \,.\, x \equiv b \; mod \; n$ tem solução se e somente se a equação diofantina $a \,.\, x + n \,.\, q = b$ tem solução, o que foi discutido 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 deste problema está em se determinar um inteiro x que satisfaça às duas congruências:

$x \equiv 1 \; mod \; 11$,
$x \equiv 2 \; mod \; 13$.

Um conjunto de congruências lineares como este é chamado de um *sistema de congruências lineares*. Para encontrar uma solução do sistema acima, basta observar que da primeira congruência temos que existe um inteiro t tal que $x = 11 \,.\, t + 1$. Substituindo x na segunda congruência, encontramos $(11 \,.\, t + 1) \equiv 2 \; mod \; 13$, donde segue, $11 \,.\, t \equiv 1 \; mod \; 13$.

Como em $\mathbb{Z}_{13}$, $(\overline{11})^{-1} = \overline{6}$, temos $t \equiv 6 \; mod \; 13$ e, então, $t = 13 \,.\, u + 6$, para u inteiro. Substituindo t em $x = 11 \,.\, t + 1$, temos $x = 143 \,.\, u + 67$ 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 que $x = 9 \,.\, t + 1$, para algum inteiro t, e da segunda, por substituição de x, $9 \,.\, t + 1 \equiv 2 \ mod\ 12$. Daí, $9 \,.\, t \equiv 1 \ mod\ 12$.

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 tais que $mdc(n_i, n_j) = 1$ para $i \neq j$. Se $a_1, a_2, ..., a_k$ são inteiros, então o sistema

$x \equiv a_1 \ mod\ n_1$
$x \equiv a_2 \ mod\ n_2$
...
$x \equiv a_k \ mod\ n_k$

tem uma única solução módulo $n_1 \,.\, n_2 \,.\, ... \,.\, n_k$.

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 $m \,.\, n$.

Da primeira equação temos que $x = n \,.\, t + a$, para algum inteiro t, e da segunda, por substituição de x, temos que $n \,.\, t + a \equiv b \ mod\ m$ ou, ainda, $n \,.\, t \equiv (b - a) \ mod\ m$.

Como $mdc(m, n) = 1$, $\overline{n}$ tem inverso em $\mathbb{Z}_m$ e, então, chamando de $\overline{i}$ o tal inverso, a solução da congruência acima é $t \equiv (i \,.\, (b - a)) \ mod\ m$.

Portanto, $t = m \,.\, u + i \,.\, (b - a)$, com u inteiro. Daí, substituindo em $x = n \,.\, t + a$, temos $x = n \,.\, m \,.\, u + n \,.\, i \,.\, (b - a) + a$ ou ainda $x = (1 - n \,.\, i) \,.\, a + n \,.\, i \,.\, b + n \,.\, m \,.\, u$.

Como, $\overline{n} \,.\, \overline{i} = \overline{1}$ em $\mathbb{Z}_m$, temos que existe um inteiro j tal que $1 - n \,.\, i = m \,.\, j$ e, então, $x = m \,.\, j \,.\, a + n \,.\, i \,.\, b + n \,.\, m \,.\, u$, com u inteiro, é solução do sistema acima.

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, $(m \,.\, n)|(x - y)$. Logo, $x_0 \equiv y_0 \ mod\ (m \,.\, n)$ e o sistema tem uma única solução em $\mathbb{Z}_{m.\,n}$.

No exemplo

$x \equiv 1 \ mod\ 11$,
$x \equiv 2 \ mod\ 13$,

discutido acima, temos $x = 13 \,.\, j \,.\, 1 + 11 \,.\, i \,.\, 2 + 11 \,.\, 13 \,.\, u = 13 \,.\, j + 22 \,.\, i + 143 \,.\, u$.

Como $1 - 11 \,.\, i = 13 \,.\, j$, é fácil determinar, pelo algoritmo de Euclides, valores para i e j. No caso, temos $i = 6$ e $j = -5$. Então, $x = 67 + 143 \,.\, u$ é solução do sistema para todo inteiro u. Tomando $u = 0$ temos que $x = 67$ é a única solução módulo $13 \,.\, 11 = 143$.

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* mxn, é a imagem de uma função f de $\mathbb{Z}_m \times \mathbb{Z}_n$ em $\mathbb{Z}$, sendo indicada por $M = (a_{ij})_{mxn}$, 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 como uma tabela (no sentido usual do termo) na qual a imagem do par (i, j) ocupa a linha i e a coluna j. Por exemplo, a matriz $M = (a_{ij})_{4x3}$ dada por $a_{ij} = i + j$ pode ser exibida da seguinte forma

$$\begin{pmatrix} 2 & 3 & 4 \\ 3 & 4 & 5 \\ 4 & 5 & 6 \\ 5 & 6 & 7 \end{pmatrix}$$

pois, $a_{11} = 1 + 1$, $a_{12} = 1 + 2 = 3$, $a_{13} = 1 + 3 = 4$, $a_{21} = 2 + 1 = 3$, e assim por diante.

O teorema do resto chinês tem uma interpretação na forma de uma matriz. Seja $M = (a_{ij})_{mxn}$ uma matriz de ordem mxn, m e n sendo inteiros tais que $mdc(m, n) = 1$. O que o teorema do resto chinês afirma é que podemos definir uma matriz definindo a_{ij}, para $i = 1, 2, ..., m$ e $j = 1, 2, ..., n$, como sendo o inteiro x tal que $1 \leq x \leq m \,.\, n$, $x \equiv i \bmod m$ e $x \equiv j \bmod n$ e que, neste caso, todos os elementos de M são distintos.

7.9 A função Φ de Euler

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, $\Phi(2) = 1$, $\Phi(3) = 2$ e $\Phi(4) = 2$, 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 $\Phi(12) = 4$, valor tirado da tabela da multiplicação em I_{12} apresentada no capítulo 3.

Na verdade, podemos estabelecer uma fórmula para $\Phi(n)$, como mostra a seguinte proposição.

Proposição 8.7

Sobre a função Φ de Euler são verdadeiras as seguintes afirmações:

a) $\Phi(p) = p - 1$ se e somente se p é primo.

b) Se p é primo e n é um inteiro positivo, então $\Phi(p^n) = (p - 1) \,.\, p^{n-1}$.

c) Se m e n são primos entre si, então $\Phi(m \,.\, n) = \Phi(m) \,.\, \Phi(n)$.

d) Se $p_1^{e_1} . \ldots . p_k^{e_k}$ é a decomposição em fatores primos de um inteiro positivo z, então $\Phi(z) = p_1^{e_1 - 1} . \ldots . p_k^{e_k - 1} . (p_1 - 1) . \ldots . (p_k - 1)$

Demonstração

a) Se $\Phi(p) = p - 1$, então $\overline{1}, \overline{2}, \ldots, \overline{p-1}$ são inversíveis e, portanto, para todo $1 < i < p$, $mdc(p, i) = 1$. Isto 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, $2 \,.\, p$, $3 \,.\, p$, ..., $p^{n-1} \,.\, p$ e, portanto, existem p^{n-1} elementos de $\mathbb{Z}_k$ não inversíveis. Daí, $\Phi(p^n) = p^n - p^{n-1} = = p^{n-1} \,.\, (p - 1)$, 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

$0 \leq x \leq m\ .n - 1$, $x \equiv i\ mod\ m$ 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 $\overline{x}$ tem inverso em $\mathbb{Z}_{m.n}$, então existe k tal que $(x\ .\ k) \equiv 1\ mod\ (m\ .\ n)$ o que implica, pela proposição 4.7, $(x\ .\ k) \equiv 1\ mod\ m$. Daí, multiplicando $x \equiv i\ mod\ m$ por k e aplicando a transitividade, temos que $(i\ .\ k) \equiv 1\ mod\ m$ e, então, $\overline{i}$ é inversível em $\mathbb{Z}_m$. Da mesma maneira se prova que se $\overline{x}$ é inversível em $\mathbb{Z}_{m.n}$, então $\overline{j}$ é inversível em $\mathbb{Z}_n$.

Reciprocamente, suponhamos que $x = a_{ij}$ e $\overline{i}$ e $\overline{j}$ são inversíveis em $\mathbb{Z}_m$ e em $\mathbb{Z}_n$, respectivamente. Sejam $\overline{i'}$ o inverso de $\overline{i}$ em $\mathbb{Z}_m$ e $\overline{j'}$ o inverso de $\overline{j}$ em $\mathbb{Z}_n$. Pelo teorema do resto chinês existe um inteiro y tal que $0 \leq y \leq m\ .\ n - 1$ com $y \equiv i'\ mod\ m$ e $y \equiv j'\ mod\ n$. Daí, segue que $(x\ .\ y) \equiv (i\ .\ i')\ mod\ m \equiv 1\ mod\ m$, esta última congruência advindo do fato de que $\overline{i'}$ é o inverso de $\overline{i}$ em $\mathbb{Z}_m$. Segue então que $m|(x\ .\ y - 1)$. Com raciocínio idêntico, prova-se que $n|(x\ .\ y - 1)$. Assim, pela proposição 2.6, $(m\ .\ n)|(x\ .\ y - 1)$, o que prova que $(x\ .\ y) \equiv 1\ mod\ (m\ .n)$ e, ainda, que $\overline{x}$ é inversível em $\mathbb{Z}_{m.n}$.

Provamos então que se $x = a_{ij}$ então $\overline{x}$ é inversível em $\mathbb{Z}_{m.n}$ se e somente se $\overline{i}$ é inversível em $\mathbb{Z}_m$ e $\overline{j}$ o é em $\mathbb{Z}_n$. Daí, $\Phi(m\ .\ n) = \Phi(m)\ .\ \Phi(n)$, pois, $\Phi(m\ .\ n)$ é o número de elementos inversíveis de $\mathbb{Z}_{m.n}$, $\Phi(m)$ é o número de elementos inversíveis de $\mathbb{Z}_m$ e $\Phi(n)$ é o número de elementos de $\mathbb{Z}_n$.

d) Segue de imediato do item (c) e da fórmula para $\Phi(p^n)$ com p primo.

Por exemplo, $\Phi(504) = \Phi(2^3\ .\ 3^2\ .\ 7) = 2^2\ .\ 3^1\ .\ 7^0\ .\ (2 - 1)\ .\ (3 - 1)\ .\ (7 - 1)$ e, então, $\Phi(504) = 4\ .\ 3\ .\ 1\ .\ 1\ .\ 2\ .\ 6 = 144$.

A função Φ de Euler é utilizada para uma generalização do pequeno teorema de Fermat para módulos compostos, como veremos a seguir. Para isto, necessitamos estabelecer o seguinte conceito.

Seja n um inteiro maior que 1. O conjunto de inteiros $S = \{a_1, a_2, ..., a_{\Phi(n)}\}$ é dito um *sistema reduzido de resíduos módulo n* se $\overline{a_1}, \overline{a_2}, \ldots, \overline{a_{\Phi(n)}}$ 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 $S = \{a_1, a_2, ..., a_{\Phi(n)}\}$ um sistema reduzido de resíduos módulo n. Se a é um inteiro tal que $mdc(a, n) = 1$, então $C = \{a\ .\ a_1, a\ .\ a_2, ..., a\ .\ a_{\Phi(n)}\}$ também é um sistema reduzido de resíduos módulo n.

Demonstração

Inicialmente, precisamos mostrar que, de fato, $|C| = |S| = \Phi(n)$. Isto não aconteceria se existissem dois inteiros positivos i e j, menores que $\Phi(n)$ e distintos, tais que $\overline{a\ .\ a_i} = \overline{a\ .\ a_j}$. Porém, se isto acontecesse, teríamos $\overline{a}\ .\ \overline{a_i} = \overline{a}\ .\ \overline{a_j}$, o que implicaria $\overline{a_i} = \overline{a_j}$, pois, como $mdc(a, n) = 1$, $\overline{a}$ 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 isto é imediato, pois

$$\overline{a\ .\ a_i}\ .\ (\overline{a})^{-1}\ .\ (\overline{a_i})^{-1} = \overline{a}\ .\ \overline{a_i}\ .\ (\overline{a})^{-1}\ .\ (\overline{a_i})^{-1} = \overline{1}$$

Teorema 3.7 (*Teorema de Euler*)

Sejam a e n inteiros, com n maior que 1 e $mdc(a, n) = 1$. Então $a^{\Phi(n)} \equiv 1\ mod\ n$.

Demonstração

Se $S = \{a_1, a_2, ..., a_{\Phi(n)}\}$ é um sistema reduzido de resíduos módulo n, então, pelo lema acima, o conjunto $C = \{a\ .\ a_1, a\ .\ a_2, ..., a\ .\ a_{\Phi(n)}\}$ também o é, já que uma das nossas hipóteses é que

$mdc(a, n) = 1$. Então $\overline{a_1} \cdot \overline{a_2} \cdot \ldots \cdot \overline{a_n} = \overline{a \cdot a_1} \cdot \overline{a \cdot a_2} \cdot \ldots \cdot \overline{a \cdot a_{\Phi(n)}}$ e, por conseguinte, $(a \cdot a_1 \cdot a \cdot a_2 \cdot \ldots \cdot a \cdot a_{\Phi(n)}) \equiv (a_1 \cdot a_2 \cdot \ldots \cdot a_{\Phi(n)}) \ mod\ n$.

Daí, aplicando sucessivamente a lei do cancelamento para congruências (o que pode ser feito pois $mdc(a_i, n) = 1$, para todo $i = 1, ..., \Phi(n)$), temos $a^{\Phi(n)} \equiv 1 \ mod\ n$, como queríamos demonstrar.

7.10 Uma aplicação: criptografia RSA

7.10.1 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.

7.10.2 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 de um par de inteiros (n, c) onde n é o produto de dois primos p e q e c é primo em relação a $\Phi(n)$. Vale lembrar que, se $n = p \,.\, q$ 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 8.7, $\Phi(n) = \Phi(p) \,.\, \Phi(q) = (p - 1) \,.\, (q - 1)$.

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 $\Phi(n)$ tal que $\overline{d}$ é o inverso de $\overline{c}$ em $\mathbb{Z}_{\Phi(n)}$. Observe que d existe, pois c foi escolhido de tal forma que $\text{mdc}(c, \Phi(n)) = 1$. 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. Este fato implica a quase impossibilidade de se determinar p e q a partir de n.

Uma pergunta que deve se estar fazendo o leitor é: se é muito difícil encontrar fatores grandes de um número grande, como se escolher primos grandes, já que a verificação de que um número é primo passa por mostrar que o número não tem fatores diferentes de um e dele mesmo? Na verdade existem métodos que verificam se um número é primo ou composto, sem fatorar o número. Estes métodos estão além do escopo deste livro, podendo o leitor interessado neles consultar [Coutinho 1997].

Exemplos

Para um primeiro exemplo, consideremos os primos $p = 97$ e $q = 53$. Temos:

$n = 97 \times 53 = 5\,141$,
$\Phi(n) = (97 - 1) \times (53 - 1) = 4\,992$,
$c = 7$ (podemos escolher $c = 7$, pois $\text{mdc}(7, 4\,992) = 1$)

Assim, (5 141, 7) é uma chave de codificação válida. Para esta 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:

$n = 127 \times 193 = 24\,511$,
$\Phi(n) = 126 \times 192 = 24\,192$,
$c = 5$ (podemos escolher $c = 5$, pois 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	

$1 = 5 - 2 \times 2 = 5 - (24\,192 - 5 \times 4\,838) \times 2$,
$1 = (-2) \times 24\,192 + 5 \times 9\,677$,
$d = 9\,677$.

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 convertidas em números inteiros. Ou seja, o sistema de codificação deve adotar uma função que faça esta 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
Código ASCII	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79

Letra	*P*	Q	R	S	T	U	V	W	X	Y	*Z*	Espaço em branco
Código ASCII	80	81	82	83	84	85	86	87	88	89	90	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 estes 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 $n = p \cdot q$ 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 $\overline{d}$ é o inverso de $\overline{e}$ em $\mathbb{Z}_{\Phi(n)}$, temos que $e \,.\, d = k \,.\, \Phi(n) + 1$, para algum inteiro k.

Agora, $Dec(Cod(z)) = Dec(z^e \bmod n) = (z^e)^d \bmod n = z^{e \,.\, d} \bmod n = z^{k \,.\, \Phi(n) + 1} \bmod n$ e, então, $Dec(Cod(z)) = (z \,.\, (z^{\Phi(n)})^k) \bmod n = z \bmod n$ = z, pois como mdc(n, z) = 1 o Teorema de Euler garante que $z^{\Phi(n)} \equiv 1. \bmod n$.

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: 173132176179186169132189179185.

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

$Cod(173) = 173^7 \bmod 5\,141 = 3\,288$,
$Cod(1\,321) = 1\,321^7 \bmod 5\,141 = 417$,
$Cod(761) = 761^7 \bmod 5\,141 = 2\,730$,
$Cod(79) = 79^7 \bmod 5\,141 = 3\,616$,
$Cod(1\,861) = 1\,861^7 \bmod 5\,141 = 361$,
$Cod(691) = 691^7 \bmod 5\,141 = 2\,142$,
$Cod(3\,218) = 3\,218^7 \bmod 5\,141 = 1\,707$,
$Cod(917) = 917^7 \bmod 5\,141 = 579$,
$Cod(91) = 91^7 \bmod 5\,141 = 2\,237$,
$Cod(85) = 85^7 \bmod 5\,141 = 283$,

Desta forma, a mensagem que seria 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 (2 117, 1 613) receba a mensagem 815#297#2067#2091#35#659#506#65. Temos

$Dec(815) = 815^{1\,613} \bmod 2\,117 = 1\,771$,
$Dec(297) = 297^{1\,613} \bmod 2\,117 = 691$,
$Dec(2\,067) = 2\,067^{1\,613} \bmod 2\,117 = 851$,
$Dec(2\,091) = 2\,091^{1\,613} \bmod 2\,117 = 321$,
$Dec(35) = 35^{1\,613} \bmod 2\,117 = 651$,
$Dec(659) = 659^{1\,613} \bmod 2\,117 = 77$,
$Dec(506) = 506^{1\,613} \bmod 2\,117 = 1791$,
$Dec(65) = 65^{1\,613} \bmod 2\,117 = 82$,

e a mensagem é

177169**185**132**165****177****179**182

M E **U** **A** M **O** R

Vale observar que os cálculos acima, aparentemente astronômicos, foram realizados por calculadoras que acompanham os sistemas operacionais de computadores mais modernos.

7.11 Exercícios

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 $\overline{i} = \overline{j}$ em $\mathbb{Z}_n$, então $mdc(i, n) = mdc(j, n)$

7.3. Mostre que adição $\overline{a} + \overline{b} = \overline{a+b}$ não está bem definida para a relação de equivalência $a \approx b$ *se e somente se a e b possuem o mesmo número de divisores primos*.

7.4. Pelo teorema 1.7 temos que se $\overline{a} \in \mathbb{Z}_n$, então $-(\overline{a}) = \overline{n-a}$. Mostre que $\overline{-a} = -(\overline{a}) = \overline{n-a}$.

7.5. Mostre que em $\mathbb{Z}_n$ $\overline{n-1}$ é sempre inversível com $(\overline{n-1})^{-1} = \overline{n-1}$.

7.6. Mostre que se p é primo, $0 < a < p$, e $(\overline{a})^{-1} = (\overline{a})$ 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 $(p - 1)! \equiv (-1) \ mod\ p$

7.10. (Considerando conhecidos os números racionais e o conceito de probabilidade) Sejam n um inteiro tal que $n = p \ . \ q$, com p e q primos e z um número inteiro aleatoriamente escolhido. Prove que a probabilidade de que $\overline{z}$ 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, a probabilidade referida acima é menor que 10^{-29} (considerando conhecidos os número 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) $5 \ . \ x + 7 \equiv 10 \ mod\ 15$.

b) $3 \ . \ x - 4 \equiv 0 \ mod\ 4$

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) $\Phi(625)$.

b) $\Phi(8!)$.

c) $\Phi(5.900)$.

7.16. 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.

7.17. Decifre a mensagem 255#245#66#235 recebida pelo usuário de chave pública (407, 13).

8. 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 $\mathbb{Z}$ o conjunto das classes de equivalências da relação $\approx$ e em $\mathbb{Z}$ 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 $\mathbb{Z}$ e em $\mathbb{N}$ e mostrar que as operações definidas acima estão bem definidas, no sentido de que somas e produtos independem de particulares representantes das classes. Porém, esta 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 $\mathbb{Z}$ 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, suponhamos que $(m, n) \cdot (p, q) = (r, r)$, com $q > p$. Daí, $(m \cdot q + n \cdot p, m \cdot p + n \cdot q) = (r, r)$ o que implica, agora nos naturais, $m \cdot q + n \cdot p + r = m \cdot p + n \cdot q + r$. Daí, utilizando o exercício 2.7, $m \cdot (q - p) = n \cdot (q - p)$ 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 $n + p \leq m + q$, $s \leq$ e $(m, n) \cdot (s, t) = (m \cdot t + n \cdot s, m \cdot s + n \cdot t)$, $(p, q) \cdot (s, t) = (p \cdot t + q \cdot s, p \cdot s + q \cdot t)$ e $(m \cdot s + n \cdot t) + (p \cdot t + q \cdot s) = (m + q) \cdot s + (n + p) \cdot t$.

Desta forma, sendo r a raiz da equação $s + x = t$ e t' a raiz da equação $r + x = t$, temos $(m \cdot s + n \cdot t) + (p \cdot t + q \cdot s) = (m + q) \cdot r' + (n + p) \cdot (s + r)$, o que implica $(m \cdot s + n \cdot t) + (p \cdot t + q \cdot s) = (m + q) \cdot (t - r) + (n + p) \cdot (s + r)$.

Daí, pelo exercício 2.8, $(m \cdot s + n \cdot t) + (p \cdot t + q \cdot s) \leq (m + q) \cdot t + (n + p) \cdot s$ o que mostra que $(m, n) \cdot (s, t) \leq (p, q) \cdot (s, t)$.

Proposição 3.8

O conjunto $\mathfrak{Z}$ 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 $S = \{(m, n) \in \mathfrak{Z} / (m, n) > (m_0, n_0)\}$. 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 $\mathfrak{Z}$ 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.

9. Os números racionais

9.1 Introdução

Os números inteiros não são suficientes para resolver todas as questões do dia a dia. Por exemplo, se uma avó pretende distribuir 15 reais com seus dois netos não existirá uma quantia inteira de reais que resolva esta questão. Ou seja, existem equações do tipo $m \,.\, x = n$, com m e n inteiros que não são solúveis, como, por exemplo, $2 \,.\, x = 5$. Neste capítulo, vamos *definir* o conjunto dos *números racionais* no qual para $m \neq 0$ a equação acima é solúvel. Para isto necessitamos definir um nova estrutura algébrica, chamada *corpo*.

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 $\overline{a}$ é inversível em $\mathbb{Z}_5$, qualquer que seja $\overline{a} \in \mathbb{Z}_5$, $\overline{a} \neq \overline{0}$. Por seu turno, $\mathbb{Z}_{12}$ não é um corpo pois, por exemplo, $\overline{6}$ 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 1.9

$\mathbb{Z}_n$ é um corpo se e somente se n é primo.

Demonstração

Se $\mathbb{Z}_n$ é um corpo, então todo elemento $\overline{a}$, 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 $\overline{a}$ um elemento não nulo de $\mathbb{Z}_n$. Seja b um representante da classe $\overline{a}$ tal que $1 < b < n$. Com n é primo, temos que $mdc(b, n) = 1$ e, então, pela mesma proposição 7.7, $\overline{b}$ é inversível. Como $\overline{a} = \overline{b}$, temos que $\overline{a}$ é inversível e $\mathbb{Z}_n$ é um corpo.

Lembremos que um anel A é um domínio de integridade se gozar da seguinte propriedade: se $a, b \in A$ e $a \,.\, b = 0$, então $a = 0$ ou $b = 0$. Por exemplo, ainda para lembrar, $\mathbb{Z}$ e $\mathbb{Z}_5$ são domínios de integridade, enquanto $\mathbb{Z}_4$ não o é, pois, neste anel, $\overline{2} \,.\, \overline{2} = \overline{0}$.

Proposição 2.9

Todo corpo é um domínio de integridade.

Demonstração

Sejam K um corpo e $a, b \in K$ tais que $a \,.\, b = 0$. Se $a \neq 0$, então existe a^{-1} tal que $a \,.\, a^{-1} = 1$. Assim, multiplicando a igualdade $a \,.\, b = 0$ por a^{-1}, temos $a^{-1} \,.\, (a \,.\, b) = a^{-1} \,.\, 0$, o que implica $b = 0$.

9.2 O corpo de frações de um domínio de integridade

Mostraremos agora que um domínio de integridade gera um corpo. Para isto seja A um domínio de integridade e consideremos o seguinte conjunto $B = \{(a, b) \in A \times A \mid b \neq 0\}$.

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 $(a, b) \approx (a', b')$, que $a \,.\, b' = a' \,.\, b$, e de $(a', b') \approx (a'', b'')$, que $a' \,.\, b'' = a'' \,.\, b'$. Multiplicando a primeira desta 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 $\boldsymbol{K}$ (ou seja, $\boldsymbol{K} = \left\{ \frac{a}{b} | a\,,\, b \in A \text{ e } b \neq 0 \right\}$.

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, $a \,.\, d = b \,.\, c$.

Definimos em K as seguintes operações:

Adição: $\frac{a}{b} + \frac{c}{d} = \frac{a \,.\, d + b \,.\, c}{b \,.\, d}$.

Multiplicação: $\frac{a}{b} \cdot \frac{c}{d} = \frac{a \,.\, c}{b \,.\, d}$.

Como fizemos em seções anteriores, é necessário que provemos que estas 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 $\boldsymbol{K}$. Para isto, 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 $b \,.\, d \neq 0$.

Para provar que os resultados independem dos representantes das classes, suponhamos $\frac{a}{b} = \frac{a'}{b'}$ e $\frac{c}{d} = \frac{c'}{d'}$. Temos que $a \,.\, b' = a' \,.\, b$ e $c \,.\, d' = c' \,.\, d$ e multiplicando a primeira destas igualdades por $d \,.\, d'$, obtemos $a \,.\, b' \,.\, d \,.\, d' = a' \,.\, b \,.\, d \,.\, d'$ e multiplicando a segunda por $b \,.\, b'$, obtemos $b \,.\, b' \,.\, c \,.\, d' = b \,.\, b' \,.\, c' \,.\, d$ que, somadas, resultam $(a \,.\, d + b \,.\, c) \,.\, b' \,.\, d' = (a' \,.\, d' + b' \,.\, c') \,.\, b \,.\, d$ e, portanto, $\frac{a \,.\, d + b \,.\, c}{b \,.\, d} = \frac{a' \,.\, d' + b' \,.\, c'}{b' \,.\, d'}$ o que mostra que $\frac{a}{b} + \frac{c}{d} = \frac{a'}{b'} + \frac{c'}{d'}$.

Deixamos como exercício mostrar que a multiplicação está bem definida.

Teorema 1.9

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 $\boldsymbol{K}$ é uma 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.

$$\begin{aligned} \frac{a}{b} \cdot \left(\frac{c}{d} + \frac{e}{f} \right) &= \frac{a}{b} \cdot \frac{c \,.\, f + d \,.\, e}{d \,.\, f} = \frac{a \,.\, c \,.\, f + a \,.\, d \,.\, e}{b \,.\, d \,.\, f} \cdot \frac{b}{b} \\ &= \frac{(a \,.\, c) \,.\, (b \,.\, f) + (b \,.\, d) \,.\, (a \,.\, e)}{(b \,.\, d) \,.\, (b \,.\, f)} = \frac{a \,.\, c}{b \,.\, d} + \frac{a \,.\, e}{b \,.\, f} \\ &= \frac{a}{b} \cdot \frac{c}{d} + \frac{a}{b} \cdot \frac{e}{f} \end{aligned}$$

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 $\frac{a}{b} \cdot \frac{b}{a}=\frac{a \,.\, b}{b \,.\, a}=\frac{1}{1}$ temos que $\frac{a}{b}$ é inversível e $\left(\frac{a}{b}\right)^{-1}=\frac{b}{a}$.

Proposição 3.9

Seja A um domínio de integridade e $\boldsymbol{K}$ o seu corpo de frações. Então, para todo $b \in A$, $b \neq 0$,

a) $\frac{a}{-b}=\frac{-a}{b}$

b) $\frac{-a}{-b}=\frac{a}{b}$

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 a ser provada 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 4.9

Sejam A um domínio de integridade e $\boldsymbol{K}$ o seu corpo de frações. Então a função $j : A \to \boldsymbol{K}$ definida por $j(a) = \frac{a}{1}$ é um homomorfismo injetivo.

Demonstração

Temos que

$$j(a + b) = \frac{a+b}{1}=\frac{a}{1}+\frac{b}{1}= j(a) + j(b),$$

$$j(a \,.\, b) = \frac{a \,.\, b}{1}=\frac{a}{1} \cdot \frac{b}{1}= j(a) \,.\, j(b)$$

e $j(1) = \frac{1}{1}= 1_K$, mostrando que j é um homomorfismo. Para mostrar que j é injetivo, suponhamos que $a, b \in A$ e $a \neq b$. Daí, $a \,.\, 1 \neq b \,.\, 1$ o que implica $\frac{a}{1} \neq \frac{b}{1}$. Logo $j(a) \neq j(b)$ e j é injetivo.

Deste modo A e $j(A)$ são isomorfos e, portanto, são algebricamente iguais Isto nos permite identificar $a \in A$ com $\frac{a}{1} \in \boldsymbol{K}$.

9.3 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, esta "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,

$$\frac{3}{4}=\left\{\ldots, \frac{-6}{8}, \frac{-3}{4}, \frac{3}{4}, \frac{6}{8}, \frac{9}{12}, \ldots\right\}$$

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 $a = b \,.\, q$, para algum inteiro *q*, de sorte que $\frac{a}{b}=\frac{b \,.\, q}{b}=q$.

No racional $\frac{a}{b}$, *a* é chamado *numerador* e *b* é chamado *denominador*. Da igualdade $\frac{a}{-b}=\frac{-a}{b}$, provada na proposição 4.9, 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 5.9

Seja um racional $\frac{a}{b}$, com $b > 0$. Então existem inteiros *a'* e *b*' tais que $mdc(a', b') = 1$ e $\frac{a'}{b'}=\frac{a}{b}$.

Demonstração

Seja $d = mdc(a, b)$. Tome, $a' = \frac{a}{d}$ e $b' = \frac{b}{d}$. Pela observação acima, *a*' e *b*' são inteiros e pelo exercício 6.4, $mdc(a', b') = 1$. Além disso, $a \,.\, b' = a'.\, d \,.\, b' = a' .\, b$ e, então, $\frac{a'}{b'}=\frac{a}{b}$.

Sejam $\frac{a}{b}$ e $\frac{c}{d}$ no corpo $\mathbb{Q}$, com $b > 0$ e $d > 0$. Definimos uma relação binária $\leq$ por

$$\frac{a}{b} \leq \frac{c}{d} \text{ se e somente se } a \,.\, d \leq b \,.\, c \text{ em } \boldsymbol{Z},$$

onde, por enquanto, o primeiro ≤ simboliza a relação que estamos definindo e o segundo a relação de ordem em $\mathbb{Z}$. 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 6.9

$\mathbb{Q}$ munido da relação definida acima é um domínio ordenado.

Demonstração

Precisamos mostrar que a relação ≤ é reflexiva, antissimétrica, transitiva, total e, ainda, é compatível com a adição e com a multiplicação.

Como $a \,.\, b \leq b \,.\, a$, 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, $a \,.\, d \leq b \,.\, c$ e $b \,.\, c \leq a \,.\, d$, em $\mathbb{Z}$. Como ≤, em $\mathbb{Z}$, é antissimétrica $b \,.\, c = a \,.\, d$ 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, $a \,.\, d \leq b \,.\, c$ e $c \,.\, f \leq d \,.\, e$. Como estamos supondo que $b > 0$ e $f > 0$, temos pela compatibilidade com a multiplicação de ≤ em $\mathbb{Z}$ que $a \,.\, d \,.\, f \leq b \,.\, c \,.\, f$ e $b \,.\, c \,.\, f \leq b \,.\, d \,.\, e$. Daí, pela transitividade de ≤ em $\boldsymbol{Z}$, $a \,.\, d \,.\, f \leq b \,.\, d \,.\, e$. Como $d > 0$, o item (b) do exercício 3.7 garante que $a \,.\, f \leq b \,.\, e$, 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 $\mathbb{Z}$, $a \,.\, d \leq b \,.\, c$ ou $b \,.\, c \leq a \,.\, d$. Daí, $\frac{a}{b} \leq \frac{c}{d}$ ou $\frac{c}{d} \leq \frac{a}{b}$.

A demonstração de que ≤ definida acima é compatível com a adição em $\mathbb{Q}$ será deixada como exercício. Para mostrar a compatibilidade com a multiplicação, sejam $\frac{a}{b}$, $\frac{a'}{b'}$, $\frac{c}{d} \in \mathbb{Q}$ tais que $\frac{a}{b} \leq \frac{c}{d}$ e $\frac{a'}{b'} \geq 0$. Assim, $a \,.\, d \leq b \,.\, c$ e $a' \geq 0$ e, então, pela compatibilidade com a multiplicação de ≤ em $\mathbb{Z}$, $a \,.\, d \,.\, a' \leq b \,.\, c \,.\, a'$. Como estamos supondo que todo denominador é positivo, pela propriedade de ≤ em $\mathbb{Z}$ e arrumando para o que queremos, $(a \,.\, a') \,.\, (d \,.\, b') \leq (b \,.\, b') \,.\, (c \,.\, a')$.

Daí, $\frac{a \,.\, a'}{b \,.\, b} \leq \frac{c' \,.\, a'}{d \,.\, b'}$ e, finalmente, $\frac{a}{b} \cdot \frac{a'}{b'} \leq \frac{c}{d} \cdot \frac{a'}{b'}$.

Sendo $\mathbb{Q}$ um domínio ordenado, podemos utilizar todas as propriedades desta estrutura algébrica obtidas no capítulo 3.

9.4 "Números" não racionais

No corpo dos números racionais toda equação da forma $a \,.\, x = b$ é solução para todo $a \neq 0$. De fato, a, sendo não nulo, possui um inverso a^{-1} e, então, multiplicando a equação por este inverso, temos $a^{-1} \,.\, (a \,.\, x) = a^{-1} \,.\, b$ 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 esta 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* $\frac{m}{n}$. Isto 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 6.9

Se p é um número primo então $\sqrt{p}$ não é racional.

Demonstração

Suponhamos por absurdo que $\sqrt{p} = \frac{m}{n}$. Pela proposição 5.9, podemos supor que m e n são primos entre si. De $\sqrt{p} = \frac{m}{n}$ segue que $p = \frac{m^2}{n^2}$ e, por conseguinte, $m^2 = p \cdot n^2$. Daí, $p|m^2$ e, portanto, $p|m$, pois p é primo. Segue então que $m = k \cdot p$, para algum inteiro k ou, ainda, $m^2 = k^2 \cdot p^2$, para algum inteiro k. Substituindo m^2 em $m^2 = p \cdot n^2$, temos que $k^2 \cdot p^2 = p \cdot n^2$ e, então, pela lei do cancelamento, $k^2 \cdot p = n^2$, o que mostra que $p|n^2$, donde segue que $p|n$. Porém esta conclusão é absurda pois, assim, p seria fator comum de m e n e estamos supondo que m e n são primos entre si.

9.5 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. 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 . 7 = 7,
2 . 7 = 14,
3 . 7 = 21,
4 . 7 = 28,
5 . 7 = 35,

e, portanto, o quociente, é igual a 4, pois 5 . 7 > 30.

Isto 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 $n \cdot q < m$
    $q := q + 1$;
$q := q - 1$;
$r := m - n \cdot q$;
escreva(q, r);

Que este algoritmo pára 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 $\lceil\ \rceil$ e assim definida $\lceil x \rceil = z$, tal que $z \leq x$ e se $m \in \mathbb{Z}$ e $m \leq x$, então $m \leq z$.

Proposição 7.9

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 $m = n \,.\, q + r$. Multiplicando esta igualdade por $\frac{1}{n}$ obtemos $\frac{m}{n} = q + \frac{r}{q}$ (lembre que $m = \frac{m}{1}$). Dai, como $n > 0$ e $r \geq 0$, temos que $\frac{m}{n} \geq q$. 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 é interrompida quando $q = \lceil \frac{m}{n} \rceil + 1$ e o comando a seguir 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 8.9

Para todo inteiro positivo m, $\lceil \frac{m}{2} \rceil \geq \frac{m}{2} - \frac{1}{2}$

Demonstração

Se m é par, $m = 2$. k, 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.

9.6 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 isto 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 $\lfloor\ \rfloor_2$ 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 9.9

A função acima definida 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 10.9

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

$a = b\,.\,q_1 + r_2, \qquad 0 \leq r_2 < b$
$b = r_2\,.\,q_2 + r_3, \qquad 0 \leq r_3 \leq r_2$
$r_2 = r_3\,.\,q_3 + r_4, \qquad 0 \leq r_4 < r_3$
. . . . .
$r_{n-1} = r_n\,.\,q_n + r_{n+1}, \qquad r_n > 0$ 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 $r_n \geq 1$, $1 \leq r_n < \frac{r_{n-2}}{2} < \frac{r_{n-4}}{2} < \ldots < \frac{r_{n-\lceil \frac{n-1}{2} \rceil}}{2^{\lceil \frac{n-1}{2} \rceil}} \leq \frac{b}{2^{\lceil \frac{n-1}{2} \rceil}}$

e, portanto $2^{\lceil \frac{n-1}{2} \rceil} < b$.

Como, por definição $b \leq \lfloor b \rfloor_2$, temos que $2^{\lceil \frac{n-1}{2} \rceil} \leq \lfloor b \rfloor_2$ e então, pela proposição anterior, $lg_2\, 2^{\lceil \frac{n-1}{2} \rceil} \leq lg_2\, \lfloor b \rfloor_2$. Daí, $\lceil \frac{n-1}{2} \rceil \leq lg_2\, \lfloor b \rfloor_b$ e, como $\lceil \frac{n-1}{2} \rceil \geq \frac{n-1}{2} - \frac{1}{2}$, temos $\frac{n-1}{2} - \frac{1}{2} \leq$ $\leq lg_2\, \lfloor b \rfloor_2$ donde segue, $n \leq 2\,.\,(1 + lg_2\, \lfloor b \rfloor_2\,)$.

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 destas 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.

9.7 Exercícios

9.1. 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 ≠ b e c ≠ d.

e) $\frac{a}{c}=\frac{b}{d}$, se c ≠ 0.

9.2. Seja *z* um inteiro positivo. Mostre que se a equação $x^2 - z = 0$ não tem solução em ℤ, então ela não tem solução em ℚ.

9.3. Mostre que a relação de ordem definida em ℚ é compatível com a soma. Isto é, prove que se $\frac{a}{b}, \frac{a'}{b'}, \frac{c}{d} \hat{I}$ ℚ e $\frac{a}{b} \le \frac{a'}{b'}$, então $\frac{a}{b}+\frac{c}{d} \le \frac{a'}{b'}+\frac{c}{d}$.

9.4. Sejam *a*, *b* ∈ ℚ, com b ≠ 0. Mostre que existe um inteiro *n* tal que $n \cdot b \ge a$.

9.5. Sejam *a*, *b* ∈ ℚ. Mostre que $a > b > 0$ se e somente se $b^{-1} > a^{-1} > 0$.

9.6. Prove que todo domínio de integridade finito é um corpo.

9.7. Mostre que quaisquer que sejam os racionais r_1 e r_2, com $r_2 \ge r_1$, existe um racional *r* tal que $r_1 \le r \le r_2$.

9.8. Mostre que o conjunto limitado inferiormente $S = \{x \in \mathbb{Q} \mid 0 < x < 1\}$ não tem elemento mínimo, o que mostra que ℚ não é um domínio bem ordenado.

10. Os números reais

10.1 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 a unidade, tem medida a tal que $a^2 = 2$. Ora, é fácil mostrar (como 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. Esta extensão deveria, naturalmente, manter as propriedades algébricas satisfeitas pelo corpo $\mathbb{Q}$.

Uma forma para construir uma tal extensão é usar um ingrediente que em Matemática mais avançada chamamos de topológico. A base do processo é caracterizar os "buracos" existentes por sequências de racionais que, num certo sentido, se acumulam em volta de cada um.

10.2 Sequência de números racionais

O conjunto $S(\mathbb{Q})$ das sequência 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 $S(\mathbb{Q})$ 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 $\mathbb{Q}$ é arquimediano (proposição 7.9). Assim, se $n > n_0$, $(1/n) < \in$. Como $0 < (1/n)$, podemos concluir que para $n > n_0$, $0 < (1/n) < \varepsilon$. Isso pode ser interpretado da seguinte maneira: a sequência $(1/n)$ fica tão pequena quanto for exigido, ou que $(1/n)$ se aproxima de zero quando n fica suficientemente grande.

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 $S_\infty = a_1/(1 - q)$. Esta fórmula decorre da observação de que na fórmula de S_n, 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 $|a_n - a| < \varepsilon$. Este elemento a é chamado *limite da sequência* e escreve-se $\lim a_n = a$.

Assim, no exemplo 1 a sequência $(1/n)$ converge para zero, enquanto que no exemplo 2, a sequência (S_n) converge para S_∞, ou seja, $\lim (1/n) = 0$ e $\lim S_n = S_\infty$.

Proposição 1.10

Se limite de (a_n) existe, ele é único

Demonstração

Sejam $\lim a_n = a_1$ e $\lim a_n = a_2$. Então, para $\varepsilon = |a_1 - a_2|/2$, 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 $\varepsilon = |a - 1|/2$ e observe que para qualquer n_o, sempre existirão infinitos índices $n > n_o$ tais que $a_n = 1$ e portanto $|a_n - a| = |1 - a| > |a - 1|/2$. Se $a \neq -1$, tome $\varepsilon = |a - (-1)|/2$ 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 2.10

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 3.10

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, $m \geq n_o$, $|a_n - a| < \varepsilon/2$ e $|a_m - a| < \varepsilon/2$. Logo $|a_n - a_m| = |a_n - a_m - a + a| \leq |a_n - a| + |a_m - a| < (\varepsilon/2) + (\varepsilon/2) = \varepsilon$.

Esta 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) onde $a_o = 0$ e $a_{n+1} = 1/(2 + a_n)$ e suponhamos que $lim\ a_n = a$. Então $lim\ (a_{n+1}) = lim\ (a_n) = lim\ (1/(2 + a_n)) = (1/(2 + \lim a_n)$. Logo, $a = (1/(2 + a))$ o que implica $(a + 1)^2 = 2$, o que não é possível com $a \in \mathbb{Q}$. Isto mostra que (a_n) não é convergente. Por outro lado,

$$| a_{n+1} - a_n | = \left| \frac{1}{2 + a_n} - \frac{1}{2 + a_{n-1}} \right| = \left| \frac{(2 + a_{n-1}) - (2 + a_n)}{(2 + a_n) \,.\, (2 + a_{n-1})} \right| = \left| \frac{a_{n-1} - a_n}{(2 + a_n) \,.\, (2 + a_{n-1})} \right| \leq \frac{1}{4} \left| a_n - a_{n-1} \right|$$

e então,

$$|a_3 - a_2| \leq \frac{1}{4}|a_2 - a_1|,$$

$$|a_4 - a_3| \leq \frac{1}{4}|a_3 - a_2| \leq \left(\frac{1}{4}\right)^2 |a_2 - a_1|$$

.

.

.

$$|a_{n+1} - a_n| \leq \left(\frac{1}{4}\right)^{n-1} |a_2 - a_1|$$

Daí,

$$|a_{n+p} - a_n| \leq |a_{n+p} - a_{n+p-1}| + \ldots + |a_{n+1} - a_n| \leq \left(\left(\frac{1}{4}\right)^{n+p-2} + \ldots + \left(\frac{1}{4}\right)^{n-1}\right)|a_2 - a_1| \leq \frac{\left(\frac{1}{4}\right)^{n-1}}{1-\frac{1}{4}}|a_2 - a_1|$$

o que mostra que a sequência (a_n) é de Cauchy, pois é fácil ver que

$$\lim \frac{\left(\frac{1}{4}\right)^{n-1}}{1-\frac{1}{4}}|a_2 - a_1| = 0$$

O exemplo acima e a proposição 2.10 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 este conjunto uma estrutura de corpo. Tal conjunto, com um certo abuso de linguagem, conterá os racionais (ver proposição 2.10) e as lacunas existentes em $\mathbb{Q}$ serão preenchidos via sequências do tipo apresentado no exemplo 4.

10.3 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 4.10

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 $n \geq n_1$, $|a_n - 0| < \varepsilon/2$ e se $n \geq n_2$, $|b_n - 0| < (\varepsilon/2)$. Então, se tomarmos $n_0 = \max\{n_1, n_2\}$ e $n \geq n_o$, então $|a_n + b_n - 0| = |a_n + b_n| \leq |a_n| + |b_n| < (\varepsilon/2) + (\varepsilon/2) = \varepsilon$, 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 $|a_n| < \varepsilon$. 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 $(a_n - b_n) \in S_o(\mathbb{Q})$. Isto 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 a relação que acabamos de definir é uma relação de equivalência. Além disso se (a_n), (b_n) e (c_n) são elementos quaisquer de $S_c(\mathbb{Q})$ 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 $(a_n \cdot c_n) - (b_n \cdot c_n) = (a_n \cdot c_n - b_n \cdot c_n) = (a_n - b_n) \cdot c_n$. Como $(c_n) \in S_c(\mathbb{Q})$ é fácil mostrar que $|c_n| < M$, para algum racional positivo M, e isso nos dá $lim\ ((a_n - b_n) \cdot c_n) = 0$, ou seja, $(a_n \cdot c_n) - (b_n \cdot c_n) \in S_o(\mathbb{Q})$.

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
$$\overline{(a_n)} \cdot \overline{(b_n)} = \overline{(a_n \cdot b_n)}$$

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, ..., 0, ...) e o elemento neutro da multiplicação é a classe $\overline{(1)}$ da sequência constante (1, 1, 1, ..., 1, ...).

A próxima proposição permite concluir que mais que um anel $\mathbb{R}$ é um corpo.

Proposição 5.10

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 q tal que $|a_n| > q$ para todo $n \geq n_0$.

Demonstração

Suponha por contradição que o resultado fosse falso. Então para cada racional positivo q e para todo natural n_0 existiria um natural m tal $m \geq n_0$ e $|a_n| < \frac{\varepsilon}{2}$. 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 $|a_n| = |a_m - a_m + a_n| \leq |a_n - a_m| + |a_m| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon$ e (a_n) pertenceria a $S_0(\mathbb{Q})$ o que é uma contradição.

Agora, considere um $a \in \mathbb{J}$, $a \neq 0$. Então $a = \overline{(a_n)}$ onde $(a_n) \notin S_0(\mathbb{Q})$. 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 $\overline{(b_n)} = \overline{\left((a_n')^{-1}\right)} = \overline{\left(\frac{1}{a_n'}\right)}$ é o inverso de a, donde concluímos que $\mathbb{J}$ é um corpo.

As proposições 2.10 e 3.10 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 $\overline{(r)} \in R$. Esta 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 lema.

Lema 1.10

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

Suponha que o resultado fosse falso. Então, para cada $\varepsilon \in \mathbb{Q}$, $\varepsilon > 0$, e $n_1 \in \mathbb{N}$, existiria $m \in \mathbb{N}$, com $m > n_1$ e $0 < a_m < \varepsilon$. Mas (a_n) é de Cauchy e, portanto, para cada $\varepsilon \in \mathbb{Q}$, $\varepsilon > 0$, existe $n_o \in \mathbb{N}$ tal que $|a_m - a_n| < \in$, se $m, n > n_0$. Assim, $|a_n| \leq |a_n - a_m| + |a_m| < 2\varepsilon$, o que significaria $a_n \in S_o(\mathbb{Q})$, contrariando à hipótese.

Dizemos que uma sequência (a_n) *possui a propriedade P* se (a_n) satisfaz às condições do lema 1.10 e deixamos para o leitor a prova do seguinte lema.

Lema 2.10

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 esta é mesmo ordem total em $\mathbb{R}$

Teorema 1.10

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, 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 mesmos 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 3.10

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

$$0 < \frac{1}{2^n} \,.\, j_n - b \leq \frac{1}{2^n} \qquad (1)$$

Ora, da demonstração do teorema 1.10, 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 $\left(\frac{j_n}{2^n} \right) \in S(Q)$, converge para a em $\mathbb{R}$

Lema 4.10

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

$\overline{a - a_1} = \overline{(0,\ a_2 - a_1,\ a_3 - a_1,\ \ldots,\ a_n - a_1,\ \ldots)}$,

$\overline{a - a_2} = \overline{(a_1 - a_1,\ 0,\ a_3 - a_2,\ \ldots,\ a_n - a_2,\ \ldots)}$,

. . .

$\overline{a - a_m} = \overline{(a_1 - a_m,\ a_2 - a_m,\ \ldots,\ a_n - a_m,\ \ldots)}$,

Como (a_n) é de Cauchy, dado $\varepsilon \in \mathbb{Q}$, $\varepsilon > 0$, existe $n_0 \in \mathbb{N}$ 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 2.10

Em $\mathbb{R}$, toda sequência de Cauchy é convergente.

Demonstração

Seja (a_n) uma sequência de Cauchy em $\mathbb{R}$ Pelo lema 3.10, 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 teremos

$$|b_n - b_m| \leq |b_n - a_n| + |a_n - a_m| + |b_m - a_m| < 3\varepsilon$$

o que mostra que (b_n) também é de Cauchy. Pelo lema 4.10, (b_n) converge para $\overline{(b_n)} = b$. Isto garante que existe $n_0 \in \mathbb{N}$ tal que $|b_n - b| < \varepsilon$, se $n \geq n_0$. Finalmente,

$$|a_n - b| \leq |a_n - b_n| + |b_n - b| < \varepsilon + \varepsilon = 2\varepsilon,$$

para todo $n \geq n_0$, o que prova que $lim\ a_n = b$.

Bibliografia

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.

Knuth, D. E., *The Art of Computer Programming*, volume 2, *Seminumerical Algorithms*. Addison-Wesley Publishing Company, USA, 1988.

Jacy Monteiro, L. H., *Elementos de Álgebra*. Ao Livro Técnico e Científico S. A., Rio de Janeiro, 1969.

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.

Lemos, M., *Criptografa, números primos e algoritmos*. IMPA (17º Colóquio Brasileiro de Matemática), Rio de Janeiro, 1989

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