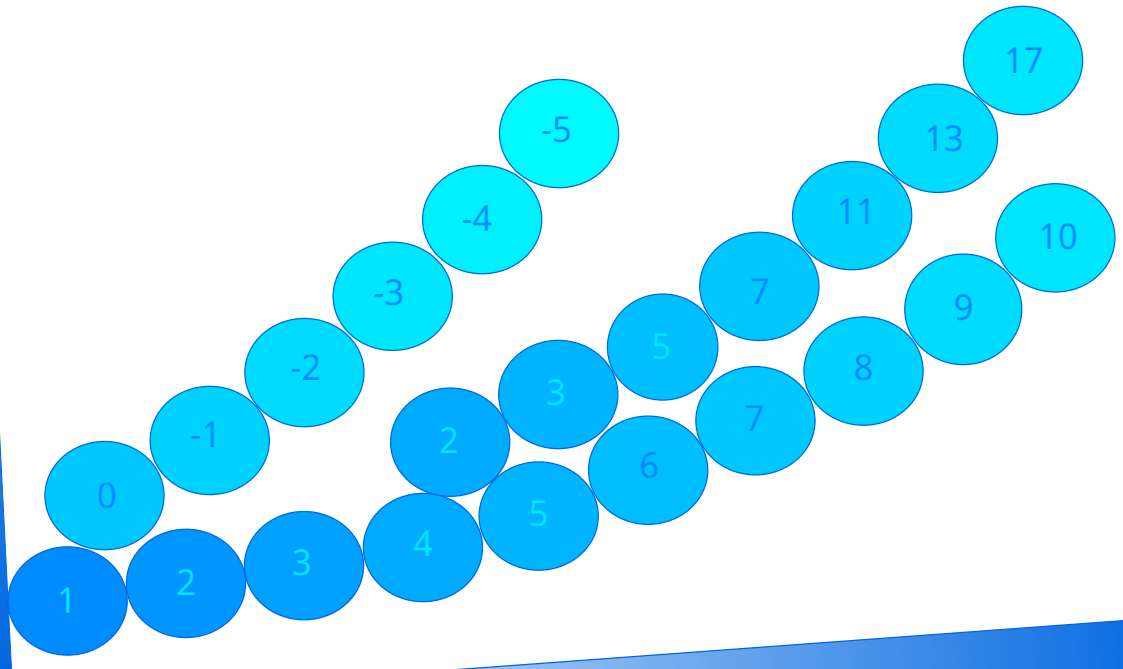
# ARITMÉTICA

# DOS NÚMEROS INTEIROS

3ª. Edição

Roberto Ribeiro Paterlini

UFSCar



# Aritmética dos números inteiros

**Roberto Ribeiro Paterlini**

3ª. edição v. $\beta$

Copyright ©2008 by Roberto Ribeiro Paterlini
Departamento de Matemática, UFSCar.

A presente versão está disponível em um arquivo em formato .pdf que pode ser acessado a partir da minha página pessoal. Mantemos seções como *Errata*, *Comentários* e *Atualizações*. A versão anterior está disponível diretamente neste endereço.

Solicitamos não disponibilizar esses arquivos em outros endereços da internet.

Este texto foi testado em sala de aula várias vezes, por mim e por colegas professores, e já foram feitas muitas correções, de modo que pensamos que está adequado para uso em cursos de formação inicial e continuada de professores de Matemática. Para sugestões ou perguntas favor se comunicar com o autor através do endereço paterlini@ufscar.br .

O *Copyright* © deste texto pertence ao autor, na forma da lei. Permito a transferência dos arquivos para uso pessoal para ledores eletrônicos ou para impressão, na forma da lei, sem qualquer ônus. Veto o uso comercial em todo ou em parte de qualquer material aqui disponibilizado, por qualquer meio. Veto modificações desse texto, sob qualquer forma. Permito que sejam feitas impressões em pequena escala por agente educacional, público ou privado, desde que o material seja distribuído gratuitamente, e não sejam cobradas taxas, nem mesmo a título de "preço de custo".

Gratos.

*Figura da capa:* Construída pelo autor com o aplicativo Inkscape. Os discos em fileiras ascendentes indicam o progresso da percepção dos números pelo homem. As cores dos discos se tornam mais claras de baixo para cima, ilustrando que essa percepção caminha do mais concreto para o mais abstrato. A lista inferior mostra os números naturais, que são a base de nossos estudos. A lista intermediária mostra os números primos, indicando os primeiros estudos da constituição quantitativa dos números naturais. A lista superior mostra o zero e os números negativos, a primeira extensão do conjunto dos números naturais. A presença da forma "disco" lembra o antigo aforisma: *O número gera a forma na matriz do espaço.*

Este texto foi editado em LaTeX 2$_\varepsilon$ pelo autor, que agradece à comunidade TeX os meios disponibilizados.

Roberto Ribeiro Paterlini

# *Aritmética dos números inteiros*

*um texto para licenciandos e professores de Matemática*



Departamento de Matemática, UFSCar.

São Carlos, Brasil.

Data da primeira edição: 25 de junho de 2008.

Terceira edição: 4 de julho de 2025.

Versão $\beta$: 24 de janeiro de 2026.

# Sumário

**Sumário** i

**Apresentação** vii

**I Aritmética dos números naturais** 1

**1 Os Números Naturais e a Arte de Contar** 3
1.1 Introdução . . . 3
1.2 Gênese dos números naturais . . . 4
1.3 Contar e representar . . . 5
1.4 O mais antigo sistema de numeração . . . 7
1.5 Sistemas primitivos de contagem . . . 8
1.6 Álgebra dos sistemas de numeração aditivos . . . 10
1.7 Sistemas de numeração aditivos históricos . . . 11
1.8 Problemas . . . 16
1.9 Sobre a gênese psicológica dos números naturais . . . 18
1.10 Sugestões de atividades . . . 19

**2 Sistemas de numeração posicionais** 21
2.1 Introdução . . . 21
2.2 Gênese dos sistemas posicionais . . . 21
2.3 Problemas . . . 24
2.4 O sistema posicional decimal . . . 24
2.5 Problemas . . . 29
2.6 Sistemas posicionais em uma base qualquer . . . 30
2.7 Problemas . . . 36
2.8 Sistemas de numeração posicionais históricos . . . 37
2.9 Pequena história do sistema de numeração decimal . . . 39
2.10 O sistema de numeração da língua portuguesa . . . 41
2.11 Os números e a legislação brasileira . . . 45
2.12 Problemas adicionais . . . 45
2.13 Sugestões de atividades . . . 48

**3 A arte de calcular** 51
3.1 Introdução . . . 51
3.2 A adição . . . 51
3.2.1 Conceito de adição . . . 52
3.2.2 Algoritmos para a adição . . . 53

3.2.3 Gênese dos algoritmos de adição para sistemas posicionais . . . . . 54
3.2.4 Problemas . . . . . 57
3.3 A subtração . . . . . 59
3.3.1 Conceito de subtração . . . . . 59
3.3.2 Algoritmos para a subtração . . . . . 61
3.3.3 Problemas . . . . . 64
3.4 Ordenação dos números naturais . . . . . 66
3.4.1 Problemas . . . . . 67
3.5 A multiplicação . . . . . 68
3.5.1 Conceito de multiplicação . . . . . 68
3.5.2 Algoritmos para a multiplicação . . . . . 70
3.5.3 Problemas . . . . . 74
3.6 A divisão . . . . . 76
3.6.1 Conceito de divisão . . . . . 76
3.6.2 Algoritmos para a divisão . . . . . 78
3.6.3 Problemas . . . . . 82
3.7 A potenciação . . . . . 83
3.7.1 Problemas . . . . . 84
3.8 Verificação de cálculos aritméticos . . . . . 85
3.9 Problemas adicionais . . . . . 86
3.10 Sugestões de atividades . . . . . 90
3.11 Temas para investigação . . . . . 92

**II Introdução à teoria dos números naturais 95**

**4 O ideal matemático da Antiga Grécia 97**
4.1 Introdução . . . . . 97
4.2 Problemas . . . . . 98
4.3 Números e Geometria . . . . . 99
4.4 Problemas . . . . . 101
4.5 Zero e os números naturais . . . . . 103
4.6 Problemas . . . . . 105
4.7 Par e ímpar . . . . . 106
4.8 Problemas . . . . . 111
4.9 Análise dos números naturais . . . . . 113
4.10 Problemas . . . . . 117
4.11 Teoria aditiva dos números naturais . . . . . 121
4.12 Problemas adicionais . . . . . 122
4.13 Pequeno exemplo de investigação . . . . . 125
4.14 Temas para investigação . . . . . 127
4.15 Sugestões de atividades orientadas . . . . . 129

**5 Números primos e compostos 131**
5.1 Introdução . . . . . 131
5.2 Propriedades dos divisores de um número natural . . . . . 131
5.3 Problemas . . . . . 135
5.4 Reconhecimento dos primos . . . . . 137
5.5 Problemas . . . . . 139

5.6 O crivo de Eratóstenes . . . 140
5.7 Problemas . . . 142
5.8 Infinitude dos primos . . . 143
5.9 Problemas . . . 145
5.10 O máximo divisor comum . . . 145
5.11 Problemas . . . 148
5.12 Algumas identidades algébricas importantes . . . 150
5.13 Problemas . . . 153
5.14 Comentários adicionais . . . 154
5.15 Problemas adicionais . . . 154
5.16 Temas para investigação . . . 158

**6 O algoritmo da divisão e aplicações 161**
6.1 Introdução . . . 161
6.2 O Teorema do Algoritmo da Divisão . . . 161
6.3 Problemas . . . 163
6.4 Existência e unicidade em sistemas posicionais . . . 164
6.5 Problemas . . . 166
6.6 Problemas adicionais . . . 166
6.7 Temas para investigação . . . 168

**7 O Teorema Fundamental da Aritmética 169**
7.1 Introdução . . . 169
7.2 Propriedades adicionais do máximo divisor comum . . . 169
7.3 Problemas . . . 171
7.4 O Teorema Fundamental da Aritmética . . . 172
7.5 Problemas . . . 173
7.6 Aplicações . . . 174
7.7 Problemas . . . 177
7.8 Os números perfeitos . . . 178
7.9 Problemas . . . 179
7.10 Problemas adicionais . . . 180
7.11 Temas para investigação . . . 182

**8 Os ternos pitagóricos 183**
8.1 Introdução . . . 183
8.2 Os ternos pitagóricos . . . 183
8.3 Problemas . . . 186
8.4 Ternos pitagóricos, o estado da arte . . . 186
8.5 Problemas . . . 188
8.6 Pierre de Fermat e seu último teorema . . . 189
8.7 Problemas adicionais . . . 189
8.8 Tema para investigação . . . 190

**III Introdução à teoria dos números inteiros 191**

**9 Os números inteiros 193**
9.1 Introdução . . . 193

9.2 A qualidade dos números negativos . . . 193
9.3 O conjunto dos números inteiros . . . 194
9.4 Problemas . . . 196
9.5 Princípios fundamentais . . . 198
9.6 Problemas . . . 199
9.7 Teoria dos números inteiros . . . 199
9.8 Problemas . . . 203
9.9 Problemas adicionais . . . 204
9.10 Temas para investigação . . . 204
9.11 Protocolo de Gauss para as congruências . . . 206
9.12 Problemas . . . 208

**10 O Método da Indução Completa 211**
10.1 Introdução . . . 211
10.2 Vale para 1, 2, 3, ..., $n$, vale sempre? . . . 211
10.3 Problemas . . . 212
10.4 O Método da Indução Completa . . . 212
10.5 Problemas . . . 216
10.6 O segundo princípio da Indução Completa . . . 217
10.7 Problemas . . . 219
10.8 Problemas adicionais . . . 220
10.9 Temas para investigação . . . 222

**11 A equação $ax + by = c$ em $\mathbb{Z}$ 225**
11.1 Introdução . . . 225
11.2 Exemplos iniciais . . . 225
11.3 O método da pulverização . . . 226
11.4 Uma fórmula para as soluções . . . 227
11.5 Problemas . . . 228
11.6 Temas para investigação . . . 230

**12 Aplicativos computacionais para TN 231**
12.1 Introdução . . . 231
12.2 Decrição sumária de alguns aplicativos . . . 231
12.3 Um pouco de TN no Maxima . . . 232
12.3.1 Exemplos em Aritmética . . . 232
12.3.2 Exemplos em TN . . . 234
12.4 Problemas . . . 236
12.5 Pequenos programas em TN . . . 236
12.6 Problemas . . . 239
12.7 Aplicativos de Inteligência Artificial . . . 240
12.8 Problemas . . . 241

**A Lista dos primos até 2500 243**

**B Respostas e sugestões a alguns problemas 245**

**C Créditos das figuras 259**

**Referências Bibliográficas** **263**

**Índice de nomes próprios** **269**

**Índice de assuntos** **271**

# Apresentação

*Meu coração propaga-se na noite.*[1]

## Sobre este texto

Este é um texto sobre Aritmética Elementar, que inclui números inteiros, sistemas de numeração, operações aritméticas, e uma introdução à Teoria dos Números. Foi escrito com a intenção de apoiar o estudo desses assuntos em cursos de formação inicial de professores de Matemática, particularmente licenciatura. A nosso ver, pode ainda ser auxílio à formação continuada.

Durante anos utilizamos anotações pessoais sobre Aritmética nos cursos de formação de professores de Matemática da UFSCar, com a ideia de que o estudo dos números é uma atividade imprescindível para sua formação e para o desenvolvimento da Matemática. Durante os anos de 2006 e 2007 nos dedicamos a revisar e ampliar essas notas e transformá-las em um livro, de modo que estudantes e professores interessados possam ter esse material à disposição.

A escolha dos assuntos aqui expostos difere em parte dos livros de Teoria dos Números escritos para o mesmo segmento de estudantes. Além dos itens de costume (divisibilidade, números primos, Teorema Fundamental da Aritmética, classes de congruências, etc.), enfatizamos bastante o estudo dos sistemas de numeração e das operações fundamentais da Aritmética e seus algoritmos. Essa opção representa a conclusão de estudos que temos feito com estudantes calouros de nossos cursos de licenciatura e com professores da escola básica em inúmeras atividades de formação continuada. O licenciando, ao realizar seus estudos como preparação para o exercício de sua profissão, necessita reconstruir seus conhecimentos em aritmética elementar sob o ponto de vista crítico da Matemática Superior. Caso contrário, se conservar como conhecimento nessa área apenas aquele que vivenciou na escola básica, tenderá a reproduzir posições cristalizadas.

## O método

Ao compor esse material acompanhamos as orientações do método *ensino da Matemática através de problemas* assim como do *método genético*. O uso de problemas como recurso didático está bem estabelecido na tradição matemática, e particularmente apreciamos a aplicação do método com o objetivo de desenvolver a arte de investigar em Matemática. Assim como aquele que investiga aprende, o que aprende deve fazê-lo praticando a arte de investigar, sem o que não é possível obter um conhecimento significativo. Para facilitar esse caminho ao estudante apresentamos um texto com muitos problemas clássicos e abertos, assim como problemas envolvendo ideias inesperadas, "fora do lugar". Às vezes repetimos problemas ao longo do texto como uma estratégia de aprendizagem. Observamos, em nossos trabalhos com estudantes,

[1] Fragmento de hino asteca.

que particularmente úteis são as seções "temas para investigação" colocadas no final de cada capítulo, a partir do terceiro.

Por outro lado, o ensino da Matemática exige também a apresentação de conceitos e ideias elaboradas ao longo da história. No meio matemático a expressão *método genético* parece ter sido utilizada pela primeira vez por Otto Toeplitz em 1926. Autor de um livro didático [117] de Cálculo Diferencial e Integral em que usou esse método, Toeplitz estava convencido de que os estudantes adquirem compreensão dos conceitos e métodos do Cálculo apenas quando se lhes apresenta sua gênese e desenvolvimento. Harold M. Edwards também utilizou o método genético em sua apresentação [33] do Último Teorema de Fermat. Segundo esse autor, a melhor maneira de superar a dificuldade em aprender uma teoria matemática abstrata é ignorar os tratados modernos até que se tenha estudado sua gênese.

Dessa forma, neste livro, a sequencialização dos assuntos tem como fio condutor a gênese dos conceitos e técnicas, e a História da Matemática é a nossa principal inspiração.

Optamos por um estilo razoavelmente detalhado e dialógico, com ampla explicação das ideias. Pensamos que dessa forma o texto poderá ser utilizado em diversas situações de ensino e aprendizagem, e o professor fica com liberdade de adotar diferentes estratégias. Particularmente apreciamos estratégias que incentivam o estudante a realizar um estudo relativamente autônomo, mais dirigido à prática da pesquisa. De qualquer forma, o que irá realmente atrair o estudante é o impulso para investigar as propriedades dos números.

### Aos estudantes, isto é, todos nós

Certamente que o estudo dos números é muito necessário para a sociedade devido às aplicações práticas e técnicas, desde as mais simples até as mais sofisticadas. Muitos ainda estudam os números por uma questão de gosto ou prazer pessoal. Pensamos que estudar os números é também uma tarefa, pois precisamos manter aceso esse conhecimento, e avançar.

### Agradecimentos

Todo o material aqui disposto foi construído através de consultas a inúmeras fontes, procuramos citá-las todas na bibliografia. Constatamos assim que participamos de uma construção coletiva. Optamos por referir no texto uma pequena parte das fontes, de outra forma iríamos sobrecarregar o estilo. Acompanhamos o costume em nossa área de não mencionar as fontes dos problemas em livros textos para estudantes.

Muito importante foi a participação dos estudantes dos cursos de Matemática da UFSCar, os quais deram o tom necessário para que este trabalho efetivamente atenda a uma necessidade. Agradecemos a atenção e envolvimento das turmas de 1995 a 2008 com as quais trabalhamos os assuntos aqui estudados. Agradecemos também às diversas turmas de professores que participaram de nossos cursos de formação continuada. Sentimo-nos verdadeiramente agraciados com as oportunidades que tivemos de contar com esses colaboradores.

Nossos agradecimentos se estendem aos colegas professores e funcionários do Departamento de Matemática da UFSCar, particularmente ao grupo de ensino da Matemática, que nos proporcionou a oportunidade de desenvolver uma clareza sobre essa importante atividade. Pensamos ser adequado citar nomes, mesmo correndo o risco de omitir alguns: Nelio Baldin, Yuriko Y. Baldin, Pedro L. A. Malagutti, Luiz J. Bettini, Yolanda K. S. Furuya, Waldeck Schützer, João C. V. Sampaio, Paulo A. S. Caetano, Jean P. Gonçalves, Fabio G. Figueira. Um agradecimento especial a Sadao Massago pela sua expertise em Latex, que me poupou muito trabalho.

Finalmente dedico esse livro aos meus familiares, com muito carinho.

São Carlos, 25 de junho de 2008. O autor.

### Observação sobre a terceira edição.

Assim como a segunda edição, esta versão incorpora correções, atualizações, acréscimos e melhoramentos. Procuramos manter uma linguagem explicativa e um diálogo claro entre o autor e o estudante. Quando possível, um triálogo, considerando também presente o futuro estudante daquele que ora pretende se tornar um professor.

Pensamos com isso estimular mais a autonomia do estudante. Nosso entendimento é que o conhecimento é construído internamente e não pode ser imposto. É preciso haver ajuda mas sem desestimular a liberdade.

Nesta terceira edição adotamos o modo hiperreferenciado do Latex. Não logramos uma programação 100% condizente, algumas ligações não conduzem à página correta. Observamos também que o comportamento desse sistema não funciona do mesmo modo em todos os ledores de pdf. Mesmo assim julgamos ser um recurso importante, de modo que resolvemos mantê-lo.

Nesta data já estamos aposentados e exercemos poucas atividades didáticas, e não dispomos de oportunidades para aplicar o texto. Assim sendo pensamos que essa terceira edição seja a última. Faremos correções à medida que recebermos contribuições. Agradecemos a oportunidade.

São Carlos, 4 de julho de 2025. O autor.

# Parte I

# Aritmética dos números naturais

# Capítulo 1

# Os Números Naturais e a Arte de Contar

*Quanto é um mais um e mais um e mais um e mais um e mais um e mais um e mais um e mais um? perguntou a Rainha Branca. — Não sei — respondeu Alice — Perdi a conta.*[1]

## 1.1 Introdução

Como surgiram os números naturais, e o que são eles?
Como o homem constrói seu entendimento desses números desde a mais tenra idade?
O que é um sistema de representação dos números naturais?
O que são os sistemas de numeração aditivos?

Apresentamos, neste capítulo, informações e reflexões sobre essas questões.

Usando sua capacidade de abstração e seu aparato lógico-dedutivo, o homem constrói o conceito do que chamamos de número natural. Essa construção é estimulada pelo meio ambiente e pela vida social. Forma-se, em cada indivíduo, um conceito, interno e residente na sua psique, abrangendo um campo que pode ser amplo ou restrito, rígido ou flexível, difuso ou preciso, o que depende de várias circunstâncias.

Nesse estudo trabalhamos com jovens que já construíram esse conceito mas que eventualmente podem expandi-lo e torná-lo mais amplo e preciso.

Por outro lado, com a finalidade de aplicar social e cientificamente o conceito de número natural, a humanidade desenvolve, desde há muito tempo, a Arte de Contar. Para isso inventou os mais diferentes sistemas de numeração, começando com os mais simples, e chegou à invenção do sistema decimal, hoje difundido em todo o mundo. Desenvolveu também muitas formas de representação dos números naturais, utilizando as linguagens falada e escrita e as linguagens simbólicas, pictográficas e de sinais.

Vejamos um pouco dessa história, e "felizes iniciemos um curso de ciência e engenhosos estudos".[2]

[1] Lewis Carrol, *Alice do outro lado do espelho* (adaptado). [19], Capítulo 9.
[2] William Shakespeare, *A Megera Domada* (adaptado). [109], Ato I, Cena I.

## 1.2 Gênese dos números naturais

Desde o alvorecer do desenvolvimento de sua autoconsciência o homem constrói o conceito de *unidade*, um segredo que se desvela paulatinamente. Aquele que designamos *número um* é um representante dessa essência, trazendo a ideia de começo. É o que inicia e dá ritmo. Revela-se, desdobrando-se, dando origem a todos os outros números, em infinitas combinações. É, ao mesmo tempo, o todo e a parte.

Do ponto de vista quantitativo, o *número um* representa a nossa percepção diante de um objeto considerado em sua unidade. Em outros termos, *um* é um conceito abstrato, representante de uma ideia universal, que construímos quando observamos, do ponto de vista quantitativo, cada objeto em sua unidade.

O número um é também chamado *unidade*.

Designamos o número um com o símbolo $1$

Desenvolvendo nossa capacidade de abstração, reconhecemos a diversidade das coisas. Observando a reunião de dois objetos, construímos o conceito do número que designamos por *dois*. Mais exatamente, *dois* é um conceito abstrato que construímos quando observamos, do ponto de vista quantitativo, um objeto reunido com outro, cada um considerado em sua unidade.

Designamos o número dois com o símbolo $1+1$

Nessa simbologia o sinal $+$ representa reunião. Traduz o movimento mental que fazemos ao reunir uma unidade com outra. Dessa forma representamos o número dois como "1 reunido com 1", ou seja, $1+1$.

Observando a reunião de três objetos, construímos o conceito do número *três*. Representamos o número três como a reunião de três unidades: $1+1+1$. Reconhecemos também que três é construído mediante o movimento de reunir uma unidade a duas unidades já reunidas, obtendo $1+(1+1)=1+1+1$, ou, de forma equivalente, $(1+1)+1=1+1+1$.

E assim, ordenadamente, construímos os números subsequentes: $1+1+1+1$ (chamado quatro), $1+1+1+1+1$ (chamado cinco), etc., sendo cada um desses números uma reunião de uma quantidade precisa de unidades.

Construímos os números com uma ordem. O número $1$ é o primeiro, o número $1+1$ é o segundo, o número $1+1+1$ é o terceiro, e assim sucessivamente. Observamos que, dado um número, o único número que lhe segue nessa ordem é obtido acrescentando-se uma unidade às unidades do número dado. Considerando o número dois e os seguintes, observamos que, dado um desses números, o número que lhe antecede nessa ordem é único.

Obtemos, dessa forma, as ideias de sucessor e de antecessor. Dado um número natural $a$, seu *sucessor* é indicado por $a+1$, e é o número construído adicionando-se uma unidade às unidades de $a$. Dado um número natural $a \neq 1$, seu *antecessor* é indicado por $a-1$, e é o número cujo sucessor é $a$. Temos a seguinte fórmula geral:

$$\underbrace{(1+1+\ldots+1)}_{a \text{ unidades}}+1=\underbrace{1+1+\ldots+1}_{a+1 \text{ unidades}}. \tag{1.1}$$

Reconhecendo que podemos repetir esse processo quantas vezes quisermos, começando com o número 1, vemos que construímos ordenadamente um conjunto infinito de números, sendo cada um deles uma reunião de uma quantidade precisa de unidades.

O conjunto dos números naturais é, portanto, o conjunto dos números

$$1, \quad 1+1, \quad 1+1+1, \quad 1+1+1+1, \quad ...$$

Estivemos estudando aspectos da origem psicológica dos números naturais. Outros detalhes serão observados na Seção 1.9, em que incluímos pequeno estudo da gênese do número na criança segundo a epistemologia genética de Jean Piaget.



## 1.3 Contar e representar

Para utilizar o conceito de número natural o homem construiu métodos de contagem.

*Contar* significa enumerar, ou relacionar sucessivamente os números naturais.[3]

Para contar necessitamos de um sistema de numeração e de uma linguagem. Um sistema de numeração provê um método de contagem, e a linguagem, uma forma de expressão.

Os sistemas de numeração são construídos das mais variadas formas.

Chamamos de *sistema de numeração* a qualquer método destinado a relacionar ordenadamente os números naturais.

Do ponto de vista da Matemática uma função básica de qualquer sistema de numeração é que ele deve determinar, implícita ou explicitamente, uma regra para o sucessor de qualquer número natural. Destacamos ainda duas importantes qualidades de um sistema de numeração: i) todo número natural tem representação no sistema; ii) a representação de qualquer número natural no sistema é única. Entretanto um sistema de numeração pode ser muito útil e não possuir essas qualidades.

Um sistema de numeração, para ter utilidade, necessita de uma linguagem para representar os números. A linguagem associa a cada número um vocábulo, um símbolo, um ícone ou um sinal. O homem inventou os mais diferentes métodos para representar os números utilizando as mais diversas linguagens, levando em conta suas necessidades de aplicação e os meios técnicos disponíveis.

Exemplos de representações de números em linguagens faladas ou escritas.

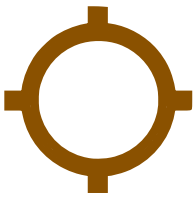
unus, duo, tres, ...
um, dois, três, ...
un, deux, trois, ...
one, two, three, ...
eins, zwei, drei, ...
iti, ni, san, ...

[3] O termo *contar* também significa verificar a quantidade de elementos de um determinado conjunto.

1 , 2 , 3 , ...
I , II , III , ...
•, ••, •••, ...
|, 𝍪, 𝍪|, ...
$\alpha$ , $\beta$ , $\gamma$ , ...
—, ═, ≡, ...

Exemplos de representações de números em linguagens simbólicas.

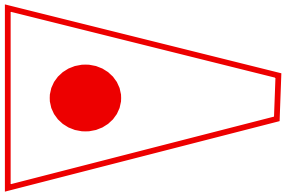
O desenho ao lado mostra o ícone para o número mil usado em Creta por volta de 1300 a.C. Esse é um exemplo de representação pictográfica.



Exemplos de representações de números em linguagens de sinais:



Representação do número 7 na Linguagem Brasileira de Sinais (LIBRAS).



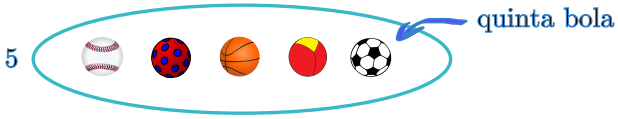
Representação do número 1 no código marítimo de sinalização.

Em Matemática, às vezes, se usa o vocábulo *numeral* para designar o nome, ou o símbolo, ou o ícone, que um número recebe em uma linguagem. Assim, um, one, unus, 𝍪, I, 1, etc, são exemplos de numerais que representam a unidade. O vocábulo *número*, por sua vez, indica a ideia abstrata. Entretanto, na linguagem escrita e falada não costumamos usar o termo numeral. Assim, dificilmente escrevemos "o número representado pelo numeral 5 é ímpar", mas sim "o número 5 é ímpar", ou mais simplesmente "5 é ímpar".

De posse de um sistema de numeração podemos contar os objetos de uma coleção, por exemplo, as bolas desenhadas abaixo. A primeira providência é estabelecer uma ordem nos objetos. Podemos fazer isso colocando-os em uma fila. Em seguida contamos: primeira, segunda, terceira, etc, apontando cada bola por sua vez. Vemos que o conjunto tem 5 bolas.



Apressamo-nos em explicar que a contagem se faz com os números ordinais: primeiro, segundo, terceiro, ..., cada um deles se refere a uma determinada bola na posição respectiva. No caso da nossa ilustração, iniciando a contagem pela esquerda, a bola de futebol tricampeã é a *quinta bola*. O número cardinal 5 corresponde, por sua vez, à totalidade das bolas na coleção.



Na linguagem comum costumamos usar os números cardinais um, dois, três, ... no lugar dos ordinais. É comum chamarmos a bola tricampeã de nossa lista de "bola cinco", o que não é formalmente correto. Um outro exemplo para explicar melhor essa questão. Dizemos por costume "hoje é trinta de janeiro", quando o correto seria "hoje é o trigésimo dia de janeiro". A palavra trigésimo se refere a um dia específico de uma lista de dias, enquanto que trinta se refere à quantidade de dias da lista até aquele dia.

## 1.4 O mais antigo sistema de numeração

A prática de esculpir entalhes em pedaços de madeira, ossos ou em paredes de cavernas, parece ter sido comum na pré-história européia, entre 35 000 e 20 000 a.C. Muitos testemunhos arqueológicos foram encontrados. Em uma escavação, realizada no território da antiga Checoslováquia, foi achado um osso de lobo no qual estão gravados 55 cortes transversais. Os 25 primeiros cortes estão agrupados de 5 em 5. Isso evidencia que se trata de um antigo registro de números. Especialistas determinaram a idade de 30 000 anos para esse achado arqueológico.

Esse registro nos sugere qual deve ter sido o mais antigo sistema de numeração utilizado por aqueles povos. Esquematizamos da seguinte forma:

| | || ||| |||| ...

As características desse sistema são:

1) Trata-se de um sistema de numeração com um único símbolo, a saber, |, representando a unidade.

2) Dada a representação de um número, para se obter a representação do sucessor basta acrescentar um símbolo |.

Denominamos a esse sistema de numeração de *sistema aditivo de base um*, ou, simplesmente, *sistema de base um*. Observe que as características descritas definem perfeitamente um sistema de numeração, pois elas nos dão uma regra para determinar o sucessor de qualquer número. Esse sistema é uma representação muito próxima da ideia da construção dos naturais, e assim tem as duas qualidades desejáveis para um sistema de numeração: todo número natural tem representação no sistema, e é única.

O sistema de numeração de base um era conveniente para o homem pré-histórico, cujas necessidades de contar eram certamente poucas. O uso desse sistema em uma civilização como a nossa traria sérios inconvenientes. Vamos apontar algumas desvantagens do sistema de base um em relação ao sistema decimal que hoje utilizamos.

a) *Reconhecimento visual de um número.* Mesmo se considerarmos valores numéricos baixos, por exemplo,

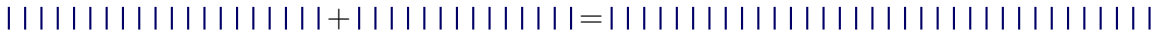
||||||||||||||||||||||||||||||||||

vemos que, para reconhecer esse número, é necessário contar a quantidade de símbolos |, e não basta olhar rapidamente para a representação. No sistema decimal a representação desse número é 34, que proporciona um reconhecimento visual imediato.

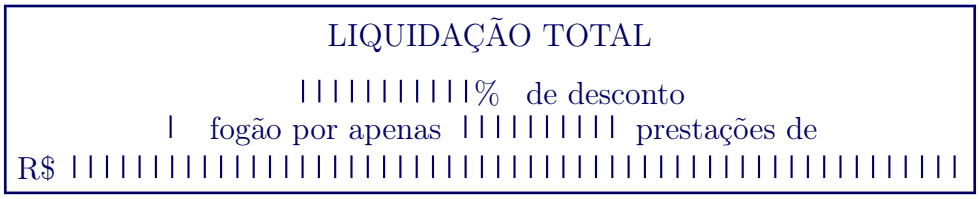
b) *Espaço ocupado pela representação.* A representação escrita de um número no sistema de base um ocupa muito espaço, mesmo para valores modestos.

c) *Implementação de algoritmos.* O sistema de base um não permite o desenvolvimento de algoritmos compactos para se efetuar as operações aritméticas. Por exemplo, a adição de dois

números deve ser feita mediante o ajuntamento dos símbolos que compõem cada um deles:



Do ponto de vista conceitual esse algoritmo é muito simples. Mas imaginemos o incômodo que teríamos se o usássemos para fazer compras ou para organizar a folha de pagamentos de salários de uma empresa.




No sistema de numeração de base um a visualização dos números pode ser melhorada se juntarmos os símbolos | em grupos de cinco, por exemplo, como o fizeram os primitivos habitantes das cavernas. Se convencionarmos que esses agrupamentos sejam indicados com a sobreposição do sinal  não é difícil ver que número está representado por



Para usar esse método precisamos saber contar e conhecer as somas $5+5$, $5+5+5$, etc.

Depois de usar muitas vezes esse estratagema, alguém pode ter tido a ideia de sintetizar a representação substituindo o símbolo  por  . Alguém pode ter usado essa mesma ideia para agrupamentos de dez unidades, e, em algum momento, o símbolo X passou a ser usado para indicar o valor dez. Seria essa a origem do algarismo romano X como símbolo do número dez?

## 1.5 Sistemas primitivos de contagem

A Etnologia é o ramo da Antropologia que estuda a cultura dos povos naturais. Certas tribos viveram isoladas durante muitos séculos, e sua cultura, às vezes bastante primitiva, foi preservada da influência da nossa civilização. Os etnólogos, ao estudar os usos, costumes e linguagens dessas tribos, descobriram os mais variados sistemas de numeração.

O estudo dos sistemas de numeração utilizados pelos povos autóctones pode ser útil de duas maneiras. Primeiro, ele nos fornece diversos exemplos de métodos de contagem. Segundo, com esse estudo podemos compreender melhor o processo cognitivo da numeração.

Indígenas da Ilhas Murray, situadas no estreito de Torres, entre a Austrália e a Nova Guiné, utilizavam os seguintes vocábulos para contar:

| | |
|---|---|
| *netat* | (um) |
| *neis* | (dois) |
| *neis netat* | (três) |
| *neis neis* | (quatro) |

Números maiores eram designados pelo vocábulo *ras*, que significava *muitos*.

Vemos aqui um sistema de numeração que utiliza basicamente os vocábulos *netat* e *neis*. Os números subsequentes são formados por combinações desses dois vocábulos. O número três é decomposto na forma $3 = 2 + 1$, e recebe o nome *neis netat*. O número quatro é decomposto

na forma $4 = 2+2$, e recebe o nome *neis neis*. Denominamos esse tipo de sistema como *sistema aditivo de base dois*.

Aparentemente os indígenas que inventaram esse sistema não precisavam de nomes para números maiores do que quatro. Mas se precisassem poderiam obtê-los seguindo sempre o mesmo método. O número cinco seria decomposto na forma $5 = 2 + 2 + 1$, e receberia o nome *neis neis netat*. O número seis seria decomposto na forma $6 = 2 + 2 + 2$, e receberia o nome *neis neis neis*. Em geral, dado um número natural qualquer $a$, podemos escrever ou $a = 2 + 2 + \ldots + 2$ ou $a = 2 + 2 + \ldots + 2 + 1$, e a denominação de $a$ nesse sistema seria *neis neis...neis* ou *neis neis...neis netat*. Portanto todo número natural tem uma e uma única representação nesse sistema.

Vemos que aqueles indígenas inventaram um sistema de numeração perfeitamente coerente. A regra do sucessor pode ser descrita da seguinte forma. Se o nome de um número termina com o vocábulo *neis*, o nome de seu sucessor se obtém repetindo-se todos os vocábulos *neis* e acrescentando-se o vocábulo *netat*. Se o nome de um número termina com o vocábulo *netat*, o nome de seu sucessor se obtém substituindo-se esse vocábulo por *neis*.

Outros indígenas das mesmas ilhas tinham um sistema semelhante:

| | |
|---|---|
| *urapon* | (um) |
| *okosa* | (dois) |
| *okosa urapon* | (três) |
| *okosa okosa* | (quatro) |
| *okosa okosa urapon* | (cinco) |
| *okosa okosa okosa* | (seis) |

Vemos que esse sistema de numeração utiliza o mesmo método do sistema anterior.

Vejamos agora um sistema um pouco diferente dos dois anteriores. Uma tribo de indígenas australianos, denominada Kamiraloi, contava da seguinte forma, em linguagem falada ([114], página 8):

| | |
|---|---|
| *mal* | (um) |
| *bulan* | (dois) |
| *guliba* | (três) |
| *bulan bulan* | (quatro) |
| *bulan guliba* | (cinco) |
| *guliba guliba* | (seis) |

Temos aqui um sistema de numeração com três vocábulos básicos: *mal*, *bulan* e *guliba*. Observe que a regra de numeração não está bem definida. Se continuarmos a contagem, vemos que oito poderá ser *bulan bulan bulan bulan* ou então *bulan guliba guliba*, ferindo a unicidade da representação. No Problema 1.8.7 o estudante é convidado a completar o estudo desse sistema.

Certos pigmeus africanos contam da seguinte forma:

| | |
|---|---|
| *a* | (um) |
| *oa* | (dois) |
| *ua* | (três) |
| *oa-oa* | (quatro) |
| *oa-oa-a* | (cinco) |
| *oa-oa-oa* | (seis) |

e assim por diante. Vemos que se trata de um sistema aditivo de base dois, com exceção do nome do número três, que é específico. Se fossem usados apenas os vocábulos *a* e *oa*, o nome do número três seria *oa-a*.

Os métodos de contagem de tribos indígenas autóctones mostram vestígios de uma época em que o homem possuia capacidade de abstração inferior à atual. Examinando os vocábulos usados para indicar números, vemos que a contagem era feita por comparação com algum conjunto mais conhecido. Assim, em certas tribos da África e do Paraguai, o número cinco era indicado por uma expressão que se pode traduzir por "os dedos de uma mão", e o número dez por "os dedos de ambas as mãos", e o número vinte por "os dedos de ambas as mãos e pés". Em certos dialetos africanos, 20 era indicado por "um homem", ou "um homem completo", e 40 por "um leito", referindo-se à reunião dos dedos das mãos e dos pés de um homem e uma mulher deitados no mesmo leito. Em alguns dialetos malaios e astecas se conta: "uma pedra", "duas pedras", "três pedras", etc, mesmo quando se está enumerando outra coisa. Analogamente, aborígenes do Sul do Pacífico dizem, para contar, "uma fruta", "duas frutas", etc., mesmo quando estão contando pedras, peixes ou outra coisa qualquer.

Em muitos dialetos, os nomes dos números são descritivos, tendo relação com um método de contar, como o uso dos dedos das mãos. No dialeto bugilai, da Nova Guiné, os nomes dos cinco primeiros números são:

| | | |
|---|---|---|
| 1 | *tarangésa* | (o dedo mindinho da mão esquerda) |
| 2 | *méta kina* | (o dedo seguinte) |
| 3 | *guigiméta kina* | (o dedo do meio) |
| 4 | *topéa* | (o dedo indicador) |
| 5 | *manda* | (o polegar) |

Em certas tribos primitivas era muito comum o uso de partes do corpo para indicar números. O etnólogo Lévy-Brühl relata que aborígenes das Ilhas Murray, no estreito de Torres, contavam até 21 usando uma correspondência com partes do corpo humano. Por exemplo, para indicar o número 11 apontavam para seu tórax. Com um procedimento semelhante, os índios papua, da Nova Guiné, contavam até 41.

O uso da base dez para contar, hoje difundido em todo o planeta, tem origem muito antiga. A ampla difusão dessa base se deve principalmente ao fato de termos dez dedos nas mãos, pois as mãos constituem o instrumento mais simples e disponível para contar. O uso dos dedos para contar certamente influenciou também a escolha das bases cinco e vinte, ou composições dessas bases. O autor W. C. Eels, investigando 306 sistemas de numeração de povos indígenas americanos, observou que 146 deles usavam a base dez, 106 usavam as bases cinco ou cinco e dez combinadas, 35 usavam as bases vinte ou cinco e vinte combinadas, 15 usavam a base quatro, 3 a base três e 1 a base oito.

Historiadores afirmam que as bases mais antigas utilizadas pela civilização foram um, dois e três, talvez devido ao fato de que esses números foram os primeiros a serem reconhecidos. Por isso, segundo esses historiadores (por exemplo, [114], página 9), não se pode afirmar que a Arte de Contar começou com o uso dos dedos das mãos. A contagem com os dedos adveio após um certo estágio de desenvolvimento.

## 1.6 Álgebra dos sistemas de numeração aditivos

Os sistemas de numeração descritos nas duas seções anteriores fazem parte de uma família mais geral, a dos sistemas aditivos. Apresentamos uma descrição algébrica desses sistemas.

Seja $\beta$ um número natural. Um *sistema aditivo de base* $\beta$ consiste de :

a) $\beta$ símbolos ou vocábulos $a_1$, $a_2$, ..., $a_\beta$ para representar os números de um a $\beta$, em ordem crescente. Os símbolos ou vocábulos escolhidos chamam-se *algarismos*.

b) regra do sucessor: se a representação de um número termina em $a_i$, para $i \neq \beta$, a representação do sucessor se obtém substituindo-se $a_i$ por $a_{i+1}$; se a representação de um número termina em $a_\beta$, a representação do sucessor se obtém acrescentando-se $a_1$ à representação dada.

Portanto, as representações dos números em um sistema aditivo de base $\beta$ são da forma $a_i$ e $a_\beta a_\beta \dots a_\beta a_i$, para $i = 1, \dots, \beta$.

A contagem nesse sistema, a partir de um, é:

$$a_1,\ a_2,\ a_3, ...,\ a_\beta,\ a_\beta a_1,\ a_\beta a_2,\ ...,\ a_\beta a_\beta,\ a_\beta a_\beta a_1,\ a_\beta a_\beta a_2, ... \tag{1.2}$$

Em um sistema aditivo a ordem de apresentação dos símbolos não precisa ser necessariamente fixada. Por exemplo, em vez de $a_\beta a_\beta a_1$ podemos escrever também $a_1 a_\beta a_\beta$ ou mesmo $a_\beta a_1 a_\beta$ sem prejuízo na indicação dos valores. Entretanto, a escolha de uma determinada ordenação dos símbolos facilita a contagem e o reconhecimento dos valores representados. Foi o que fizemos na regra do sucessor definida no item b) acima.

**Problema resolvido 1.1.** Utilize os seguintes símbolos para um sistema aditivo de base cinco: $\diamondsuit$, $\natural$, $\nabla$, $\varnothing$ e $\heartsuit$, nessa ordem. Qual é a representação do número quarenta e três nesse sistema?

*Solução.* A decomposição aditiva de 43 em grupos de 5 unidades é: $43 = 5+5+5+5+5+5+5+5+3$. Portanto sua representação no sistema dado é:

$$\heartsuit\heartsuit\heartsuit\heartsuit\heartsuit\heartsuit\heartsuit\heartsuit\nabla$$

**Problema resolvido 1.2.** Assuma que, em um sistema aditivo de base quatro, os algarismos são $\alpha$, $\beta$, $\gamma$ e $\delta$, nessa ordem. **a)** Conte de um a quinze nesse sistema. **b)** Qual é a representação do número vinte e três nesse sistema? **c)** Que número está representado por $\delta\delta\delta\delta\beta$ ? **d)** Levando em conta que, numa determinada representação, a ordem dos algarismos não importa, que número está representado por $\alpha\beta\gamma\delta$ ?

*Soluções.* a) $\alpha$, $\beta$, $\gamma$, $\delta$, $\delta\alpha$, $\delta\beta$, $\delta\gamma$, $\delta\delta$, $\delta\delta\alpha$, $\delta\delta\beta$, $\delta\delta\gamma$, $\delta\delta\delta$, $\delta\delta\delta\alpha$, $\delta\delta\delta\beta$, $\delta\delta\delta\gamma$. b) A decomposição aditiva de 23 em grupos de 4 unidades é: $23 = 4+4+4+4+4+3$. Portanto sua representação no sistema dado é: $\delta\delta\delta\delta\delta\gamma$. c) $\delta\delta\delta\delta\beta = 4+4+4+4+2 = 18$. d) A representação dada não pertence ao sistema. Toda representação desse sistema é constituída por um único algarismo, uma repetição de algarismos $\delta$ ou por um algarismo $\delta$ ou uma repetição deles ajuntado com um único dos símbolos $\alpha$, $\beta$ e $\gamma$.

## 1.7 Sistemas de numeração aditivos históricos

O método aditivo foi utilizado por muitos povos antigos para representação dos números naturais. Vejamos um pouco dessa história.

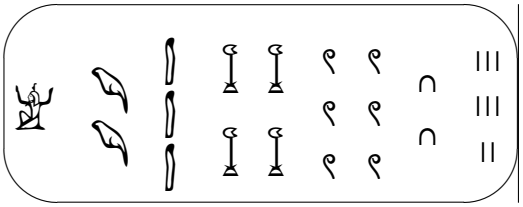
### O sistema hieroglífico egípcio

O *sistema hieroglífico egípcio* foi desenvolvido no antigo Egito a partir de 3400 a.C., pelo menos. Usado principalmente nos monumentos de pedra, seus símbolos, denominados hieróglifos, eram considerados sagrados. A base principal do sistema era 10, e as bases secundárias eram $10^2$, $10^3$, $10^4$, $10^5$ e $10^6$.

Vemos a seguir os glifos[4] para esses números.




Para representar um número natural os egípcios o decompunham aditivamente em grupos de unidades, dezenas, centenas, etc., repetindo os símbolos correspondentes até nove vezes. Por exemplo, o número 1 234 628 era decomposto na forma $1 \times 1\,000\,000 + 2 \times 100\,000 + 3 \times 10000 + 4 \times 1000 + 6 \times 100 + 2 \times 10 + 8$, de modo que sua representação era



Como o sistema não era posicional, variava muito a forma com que os símbolos eram dispostos. No exemplo acima começamos com o agrupamento de maior valor, mas os egípcios usavam também colocar à esquerda o agrupamento de menor valor.

Os antigos egípcios tinham outros dois sistemas de numeração, derivados dos sistemas de escrita cursiva usados em papiros, chamados sistemas *hierático* e *demótico*.



Figura 1.1. Detalhe do papiro Rhind, adquirido em Tebas, Egito, pelo advogado escocês Alexander Henry Rhind, aproximadamente em 1850. Foi datado como sendo de 1650 a.C. Contém 85 problemas elementares de Matemática e sua solução. Nele o escriba Ahmose (ou Ahmes) diz que o copiou de uma fonte ainda mais antiga.

## Sistemas de numeração da Antiga Grécia

No início de sua civilização os gregos utilizaram o sistema de numeração denominado *ático*, ou *herodiânico*. Foi desenvolvido provavelmente no Século VII a.C. Os símbolos para 5, 10, 100, 1000 e 10000 eram formados pelas letras iniciais dos nomes dos números. Os símbolos para 50, 500, 5000 e 50000 consistiam de uma combinação dos primeiros. Vemos abaixo uma possível representação para esses números.




[4] Glifos são pictogramas gravados em pedras.

Para representar um número natural, seu valor era decomposto aditivamente de forma a otimizar o uso dos símbolos acima. Exemplos:

27 = 𐅃𐅃𐅂𐅁𐅁 700 = 𐅆𐅆𐅇𐅇

90 = 𐅆𐅃𐅃𐅃𐅃 45000 = 𐅉𐅉𐅉𐅉𐅆𐅂

Por volta de 450 a.C. os gregos passaram a usar um sistema de numeração alfabético, denominado *jônico*. Eram emprestadas as letras do alfabeto para designar os números de 1 a 9, depois as dezenas e as centenas, conforme a tabela a seguir.

| | | | | | |
|---|---|---|---|---|---|
| 1 | Α | 10 | Ι | 100 | Ρ |
| 2 | Β | 20 | Κ | 200 | Σ |
| 3 | Γ | 30 | Λ | 300 | Τ |
| 4 | Δ | 40 | Μ | 400 | Υ |
| 5 | Ε | 50 | Ν | 500 | Φ |
| 6 | Ϝ | 60 | Ξ | 600 | Χ |
| 7 | Ζ | 70 | Ο | 700 | Ψ |
| 8 | Η | 80 | Π | 800 | Ω |
| 9 | Θ | 90 | ϙ | 900 | Ϡ |

Os caracteres exibidos nesta seção foram desenhados a partir de inscrições de antigos escritos gregos. Estão disponíveis em [128], *Greek numerals*. Esses símbolos, em geral, pertencem ao alfabeto grego, com exceção de alguns caracteres, que foram emprestados de outros alfabetos orientais.

No sistema jônico alguns números eram representados por mais de um símbolo, por exemplo, 900 também tinha a representação ϡ

A representação dos números naturais nesse sistema seguia o método aditivo. Exemplos:

37 = ΛΖ 853 = ΩΝΓ

Os milhares, a princípio, eram representados por uma combinação do milhar com o símbolo 𐅄 Por exemplo, $^{\beta}$𐅄 indicava 2000. Posteriormente se usou ,A para 1000, ,B para 2000, ,Γ para 3000, etc.

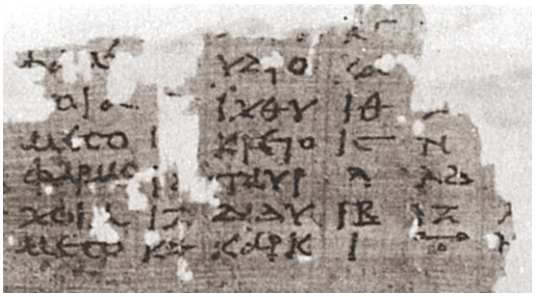


Figura 1.2. Foto de manuscrito grego do Século II cotado do artigo *Greek Numerals* em `https://en.wikipedia.org/wiki/Greek_numerals` Nessa época alguns astrônomos e estudiosos usavam o sistema sexagesimal sumério adaptado com símbolos do alfabeto grego. O zero era representado pela letra o conforme aparece no lado direito inferior do manuscrito. Esse sistema foi usado a partir do Século II a.C. por astrônomos e matemáticos, como Hiparcos de Nicea (c. 140 a.C.), Claudio Ptolomeu (c. 140), Theon de Alexandria (c. 380) e sua filha Hipacia de Alexandria (c. 400), cuja morte marcou o fim da Antiguidade Clássica.

A História da Matemática registra que vários povos adotaram sistemas numéricos denominados *alfabéticos*, assim chamados por usarem letras do alfabeto para representar números. Além dos antigos gregos, podemos citar os sistemas Abjad, o Armênio, o hindu Aryabhata, o Cirílico, o Georgiano, o Hebreu e o Romano.



Figura 1.3. O uso de um sistema numérico alfabético permanece até hoje na tradição judaica. Vemos ao lado uma foto de um relógio de bolso do Século XX com numerais representados por letras do alfabeto hebraico. Cotado de *Hebrew numerals* em `https://en.wikipedia.org/wiki/Hebrew_numerals` .

## O sistema de numeração romano

O sistema de numeração romano foi extensamente adotado na antiga Europa devido à sua simplicidade e à expansão do império romano. Desenvolveu-se a partir do Século III a.C., e foi utilizado na Europa até o Século XVI. Ainda é adotado em nossos dias para fins decorativos e para certos tipos de enumeração, como capítulos de livros, séculos, sequências de reis e papas, etc. A forma com que o utilizamos hoje segue **geralmente** as regras que descrevemos a seguir (escrevo "geralmente" porque não existe nenhuma obrigatoriedade de regras para o uso atual do sistema romano).

O sistema numérico romano adota agrupamentos aditivos de unidades, dezenas, centenas e milhares. Para evitar a repetição excessiva de símbolos são aplicados numerais intermediários para 5, 50 e 500. Pelos símbolos se vê que se trata também de um sistema alfabético:

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 1 | I | 5 | V | 10 | X | 50 | L |
| 100 | C | 500 | D | 1000 | M | | |

Também são adotados os seguintes agrupamentos subtrativos, que permitem uma economia na representação:

| | | | | | |
|---|---|---|---|---|---|
| 4 | IV | 9 | IX | 40 | XL |
| 90 | XC | 400 | CD | 900 | CM |

Na representação de um número os símbolos V, L e D nunca são repetidos, e I, X, C e M não são repetidos mais do que três vezes. A escrita dos números é feita da esquerda para a direita, isto é, o símbolo ou agrupamento de maior valor vem à esquerda do de menor valor. Quando necessário pode ser colocado um traço horizontal sobre um símbolo, um agrupamento ou um conjunto de símbolos, o que tem efeito de multiplicar por mil seu valor.

Observe que **não** são utilizados agrupamentos subtrativos como (IL) para 49, (IC) para 99, etc. Os agrupamentos subtrativos se limitam aos descritos acima.

Exemplos de números representados no sistema romano:

| | | | | | |
|---|---|---|---|---|---|
| 8 | VIII | 14 | XIV | 19 | XIX |
| 59 | LIX | 449 | CDXLIX | 1989 | MCMLXXXIX |
| 3562 | MMMDLXII | 4719 | $\overline{\text{IV}}$DCCXIX | | |

Não deve o estudante pensar que os sistemas numéricos utilizados por civilizações antigas tinham a uniformidade que nossa apresentação possa sugerir. Pelo contrário, esses sistemas passaram por inúmeras modificações, e nem sempre atingiram uma forma única.

Um exemplo típico é o sistema numérico romano. Nesse período houve muitas variações tanto no desenho dos símbolos quanto na metodologia da representação. Agrupamentos subtrativos nem sempre foram utilizados. Mesmo no Século XVI se encontram números como Mcccccxxxxviiij (1549), em que o i e o j representam a unidade. Muitas vezes a forma IIII foi preferida à forma IV, e VIIII a IX. O número 19 era em geral representado por XIX, mas às vezes também por IXX. Encontram-se também IIX para 8 e IIXX para 18. O traço horizontal sobreposto aos símbolos eram muitas vezes usados para distinguir um número de um vocábulo com a mesma grafia. Mesmo na Idade Média o traço era mais utilizado para diferenciar números de palavras do que para indicar multiplicação por mil.

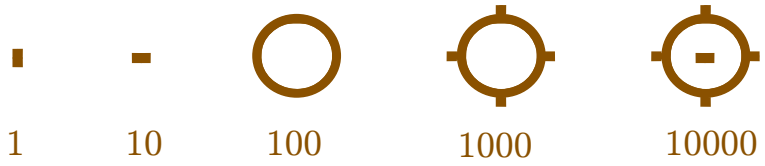
Observamos também que o uso de agrupamentos subtrativos não foi uma invenção romana. Os sumérios os utilizavam 3000 anos antes de Cristo, assim como os etruscos, que precederam os romanos na Itália.



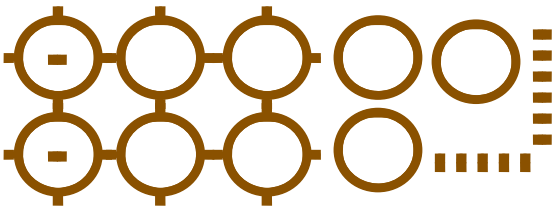

Figura 1.4. Moeda espanhola de prata do tempo do Rei Carlos IV. Observe no lado esquerdo o uso do numeral IIII em vez de IV. Cotado de *Roman numerals* em `https://en.wikipedia.org/wiki/Roman_numerals` .

## O sistema minóico

Um sistema de numeração da antiga civilização minóica, que se desenvolveu na ilha de Creta, constitui um belo exemplo de uso de linguagem pictográfica. No estágio final de seu desenvolvimento, ocorrido entre 1350 e 1200 a.C., os símbolos utilizados eram:




Os números eram decompostos aditivamente conforme o exemplo abaixo:



em que está representado $2 \times 10000 + 4 \times 1000 + 3 \times 100 + 6 \times 10 + 5 = 24365$.



Figura 1.5. Tablete encontrado em Knossos, Creta, com glifos cretenses datados de 1900-1600 a.C. Exposto no Museu Arqueológico de Heraklion, Grécia.

## 1.8 Problemas

**Problema 1.8.1.** "Contar", no âmbito da Aritmética, significa (assinale V ou F dentro dos parêntesis se a afirmação for verdadeira ou falsa, respectivamente):

( ) Construir símbolos ou vocábulos para representar os números em uma linguagem.

( ) Enumerar, ou relacionar sucessivamente os números naturais.

( ) Saber distinguir número de numeral.

( ) Ler uma história para crianças antes delas adormecerem.

( ) Saber a diferença entre número cardinal e número ordinal.

**Problema 1.8.2.** Qual o significado do verbo contar utilizado na seguinte frase: "Até os cabelos da vossa cabeça estão todos contados. Não temais ..." ([69], 12:7).

**Problema 1.8.3.** Um jovem pastor de ovelhas traz consigo uma coleção de pedrinhas cujo número é igual ao de ovelhas de seu rebanho. Como ele pode utilizar as pedrinhas para conferir a quantidade de ovelhas ao fim de um dia de pastoreio? Precisa ele saber contar? Você chamaria a esse processo de sistema de numeração?

**Problema 1.8.4.** Todas as sentenças abaixo são verdadeiras. Em cada caso, diga se estamos falando de número ou de numeral.

**a)** 3 é 3/4 de 8.

**b)** 9 é maior do que 5.

**c)** **v** é a metade de X.

**d)** 6 é menor do que 4.

**Problema 1.8.5.** O texto informa que o mais antigo sistema de numeração utilizado pelo homem seria, em símbolos:

$$| \quad || \quad ||| \quad |||| \quad \ldots$$

Considere as seguintes afirmações sobre esse sistema. Assinale V ou F dentro dos parêntesis se a afirmação for verdadeira ou falsa, respectivamente

( ) Esse sistema é matematicamente incorreto para números grandes.

( ) Nesse sistema qualquer número natural pode ser representado de forma única.

( ) O sistema é bom mas não pode ser utilizado hoje em dia pois não permite fazer divisão.

( ) É possível realizar nesse sistema todas as operações aritméticas, embora seja incômodo.

( ) Esse sistema é correto e simples mas não o utilizamos hoje em dia porque, dentre outros motivos, ele permite um reconhecimento visual imediato apenas para números com valores muito baixos.

( ) Definitivamente não podemos fazer potenciação nesse sistema de numeração pré-histórico.

**Problema 1.8.6.** Estude as seguintes questões, relativas ao sistema "urapon, okosa" utilizado pelos indígenas das Ilhas Murray, conforme descrito na Seção 1.5. **a)** continue a contagem até vinte; **b)** quais são os vocábulos básicos? **c)** qual é a regra do sucessor? **d)** liste as vantagens e desvantagens desse sistema em relação ao nosso sistema de numeração decimal.

**Problema 1.8.7.** Na contagem dos Kamiraloi, descrita na Seção 1.5, faça a seguinte modificação: coloque $4 = 1 + 3 =$ mal guliba. Observe que está agora bem definida uma regra de numeração. Continue a contagem até vinte. Descreva a regra do sucessor.

**Problema 1.8.8.** Analise o seguinte sistema de numeração, utilizado por uma tribo de indígenas australianos, que vivem nas proximidades do Rio Murray ([114], página 8):

| | |
|---|---|
| enea | (um) |
| petcheval | (dois) |
| petcheval enea | (três) |
| petcheval petcheval | (quatro) |

**Problema 1.8.9.** Imagine que você esteja vivendo por algum tempo em uma tribo de indígenas primitivos, com o intuito de estudar sua cultura. A certa altura você descobre que eles usam muitos vocábulos para indicar números, alguns deles você consegue traduzir como sendo "um homem", "dois homens" e "três homens". Que hipóteses você poderia fazer sobre os valores desses números?

**Problema 1.8.10.** O Siríaco é uma linguagem derivada do Aramaico, e foi utilizada por pequenos grupos humanos na Europa Oriental nos primeiros séculos da Era Cristã. Em uma forma antiga do alfabeto siríaco era utilizado o símbolo $|$ para indicar a unidade, e o símbolo $\cup$ para o número dois. O sistema de numeração era aditivo de base dois:

$$|,\ \cup,\ \cup|,\ \cup\cup,\ \cup\cup|, \ldots$$

**a)** Continue a contagem do sistema siríaco até vinte; **b)** dê a regra do sucessor; **c)** seria viável para nossa civilização utilizar o sistema siríaco?

**Problema 1.8.11.** Perguntaram à pequena Ana quantas maçãs tinha sua irmã mais velha. Depois de contar, ela disse: — É preciso um dedinho do pé.

Qual era a provável quantidade de maçãs da irmã de Ana?

**Problema 1.8.12.** Na história do gigante do feijoeiro, Joãozinho o escutou contando seus ovos de ouro: fee, fie, foe, fum, fot, feefot, fiefot, foefot, fumfot, fotfot, feefotfot,...

Continue a contagem. Que sistema de numeração é esse? Descreva as limitações desse sistema.

**Problema 1.8.13.** Considerando o sistema numérico do gigante do feijoeiro, escreva uma regra que permita decidir quando um número é maior do que outro.

**Problema 1.8.14.** Utilize os seguintes símbolos para um sistema aditivo de base quatro: 1, 2, 3 e 4, nessa ordem. Qual é a representação do número trinta e oito nesse sistema?

**Problema 1.8.15.** Invente um sistema aditivo de base seis, usando símbolos do tipo $\triangle$, $\oplus$, $\boxminus$, etc. Conte de um a trinta nesse sistema. Descreva a regra do sucessor.

**Problema 1.8.16.** Argumente a respeito de que todo sistema de numeração aditivo de base $\beta$ satisfaz às propriedades fundamentais de existência e unicidade.

**Problema 1.8.17.** Foi observado na Seção 1.4 que o sistema de numeração pré-histórico aditivo de base um, que usa o símbolo |, embora muito simples, não é usado hoje em dia. Dentre outros motivos isso ocorre pelo fato de que não permite o desenvolvimento de algoritmos compactos para se efetuar as operações aritméticas. O texto faz uma observação sobre a adição. Como podem ser efetuadas as outras operações nesse sistema?

**Problema 1.8.18.** Verifique se o sistema de numeração romano satisfaz às propriedades fundamentais de existência e unicidade.

**Problema 1.8.19.** Suponha que no sistema hieroglífico egípcio e no sistema minóico cada símbolo não pode ser repetido mais do que nove vezes na representação de um número. Calcule qual é o maior número natural que pode ser representado em cada um desses sistemas.

**Problema 1.8.20.** A princípio desenvolvemos um sistema de numeração para contar objetos em um conjunto. Por exemplo, se em uma cesta tivermos maçãs, podemos contá-las usando algum sistema de numeração. Na ação física de efetuar a contagem, existe uma certa escolha. Escolhemos qual é a primeira maçã, e dizemos "um" (ou outro nome). Escolhemos outra maçã para ser a segunda, e dizemos "dois", e assim por diante. A quantidade de maçãs naquela cesta depende dessas escolhas? A quantidade pode mudar se fizermos escolhas diferentes? Justifique sua resposta.

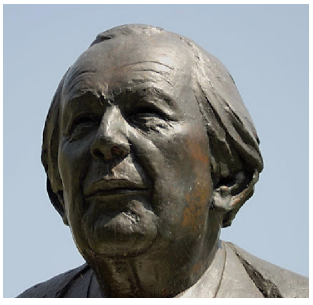
**Problema 1.8.21.** Procure explicar o sentido da palavra "infinito" usada no final da página 4.

**Problema 1.8.22.** Uma criança lhe pergunta o que é "um milhão" (referindo-se ao número). Imagine um diálogo que você possa desenvolver com ela para lhe explicar isso.

## 1.9 Sobre a gênese psicológica dos números naturais

Observações do comportamento das crianças sugerem que ela constrói pouco a pouco o conceito de número natural.

Jean Piaget, cientista suiço, especialista em psicologia do desenvolvimento. Criou a epistemologia genética, que estuda o conhecimento a partir de sua história e da psicologia.



A epistemologia genética estuda a origem e a natureza do conhecimento construído pelo homem. Jean Piaget e seus colaboradores investigaram extensamente esses assuntos, particularmente através da observação das respostas de crianças de diversas idades ao serem estimuladas por experimentos a elas apresentados. Com relação à construção do número os autores de [99] observam que não é suficiente que a criança saiba relacionar verbalmente nomes de números para que ela esteja na posse do conceito. É necessária uma construção interna realizada por seu aparato lógico-matemático mediante a superação de esquemas sucessivos, cada um dependente de um certo amadurecimento de seu sistema nervoso e estimulada por interações com o meio físico e social.

Lê-se em [58], página 19 e seguintes, que o aparato psíquico do homem obtém conhecimento através de dois tipos de abstração, a empírica e a reflexiva. A primeira nos permite reconhecer propriedades físicas nos objetos e fenômenos, como cor e peso. A segunda nos leva a criar comparações e observar relações entre objetos, como diferença e semelhança. Essas relações não são propriedades dos objetos, mas um conhecimento lógico-matemático que impomos a eles.

Quanto à aquisição do conceito de número, existem três esquemas principais que a criança precisa superar: a conservação, a síntese da ordem e a inclusão hierárquica.

A conservação, que no contexto dos números é a conservação das quantidades discretas, é a habilidade de perceber que uma quantidade de objetos (vistos como unidades) não muda se o arranjo em que elas se encontram for modificado. A síntese da ordem ocorre quando a criança sente a necessidade lógica de ordenar mentalmente os objetos de um conjunto, criando uma lista em que se tem o primeiro objeto, o segundo, etc, sem repetir e sem que nenhum objeto fique fora da lista. Por outro lado a inclusão hierárquica significa a habilidade de perceber cada número como um todo, de modo que um está incluído em dois, dois em três, e assim por diante. Esses esquemas sugerem que a adição faz parte da construção do número desde o seu início.

A aquisição do conceito de número natural é um processo bastante complexo (e não completamente compreendido), mas se sabe que aos 7/8 anos o raciocínio da criança se torna suficientemente flexível e ela adquire por si mesma o conceito de número natural.

As ideias da epistemologia genética influenciam algumas metodologias para o ensino da Matemática, dentre elas o método denominado construtivista. A principal característica dessas metodologias é promover a aprendizagem autônoma.

O que mais me surpreende é: se cada indivíduo constrói internamente os números naturais, como esse conceito parece ser bastante similar em milhões de indivíduos, talvez em bilhões? A ação do meio ambiente e social é suficiente para explicar esse fenômeno? Talvez tenhamos que considerar que no substrato cósmico age um tipo de *campo numérico*, à semelhança do campo gravitacional ou do campo morfogenético, e que nossa psique é fortemente influenciada por esse campo.

## 1.10 Sugestões de atividades

**Atividade 1.10.1.** Observando os usos e costumes de nossa sociedade, descreva situações em que o sistema de numeração aditivo de base um ainda é utilizado. E quanto a agrupamentos de cinco em cinco, ou seis em seis, de |?

**Atividade 1.10.2.** Pensa-se que a base doze deve ter sido utilizada por povos antigos do continente europeu devido aos resquícios de contagem que dela temos até hoje. Observando os

usos e costumes de nossa sociedade, assim como a história da civilização, descreva situações em que a base doze foi usada ou ainda é usada, ou está em desuso.

**Atividade 1.10.3.** Estar de posse do conceito de número não significa que possamos contar qualquer coleção de objetos. Dê exemplos de situações em que isso ocorre.

**Atividade 1.10.4.** Obtenha mais informações sobre a Língua Brasileira de Sinais (LIBRAS), particularmente sobre os sinais utilizados pelos surdos-mudos para representar números.

**Atividade 1.10.5.** Faça uma relação mais completa do que a do texto sobre representações escritas e faladas de números em diversas línguas.

**Atividade 1.10.6.** Os analfabetos, às vezes, desenvolvem sistemas próprios de contagem. Entrevistando essas pessoas, descreva métodos de contagem diferentes do nosso sistema usual. Esperamos que o estudante tenha dificuldade em encontrar pessoas analfabetas!

**Atividade 1.10.7.** O valor máximo atingido pelo sistema de contagem de um povo ou civilização depende de suas necessidades, de seus usos e costumes, e também de seu desenvolvimento científico e tecnológico. Faça uma pesquisa sobre esse tema. Sugerimos os seguintes itens:

a) Pesquise os valores numéricos usados por alguma civilização antiga, como os romanos do tempo de Cristo, por exemplo.

b) Pesquise os valores numéricos médio e máximo usados nas diversas atividades de nossa sociedade: comércio, sistema financeiro, demais organizações sociais, Astronomia, Física, Matemática, Química, e outras ciências.

**Atividade 1.10.8.** Usando um dicionário da língua portuguêsa estude o significado das seguintes palavras utilizadas neste capítulo: pictográfico, pictograma, ícone, símbolo, linguagem, conceito, abstração, autoconsciência, essência, paulatinamente, etnologia, antropologia, resquício. Descubra o que é escrita cursiva.

**Atividade 1.10.9.** Procure informações em livros, artigos ou na internet sobre métodos de numeração de povos indígenas brasileiros. Por exemplo, lendo *Quando* $1+1 \neq 2$ *in* [40], pode-se ver como indivíduos de vários povos que vivem no Parque Indígena do Xingu aprendem aritmética na Escola Diauarum, e têm suas próprias concepções sobre diversos conceitos.

**Atividade 1.10.10.** Leia um resumo da história das principais civilizações que usaram sistemas de numeração aditivos ou alfabéticos, como os cretenses, os egípcios, os gregos e os romanos. Faça uma linha de tempo localizando seus sistemas de numeração.

**Atividade 1.10.11.** Use a internet ou outras fontes para obter informações sobre registros rupestres de números na Serra da Capivara, Piauí, Brasil, a maior concentração de sítios arqueológicos das Américas. Pesquise também sobre esse tipo de registro em outros locais do mundo. Inclua uma pesquisa sobre os mais antigos registros arqueológicos sobre números. Quais sistemas de numeração podem ser identificados? Faça um resumo de suas pesquisas.

**Atividade 1.10.12.** Em várias línguas termos ou sufixos relacionados com os números 3 e 4 indicam "muitos", ou "multidão", um resquício do uso desses números em sistemas de numeração primitivos. Faça uma pesquisa sobre esse assunto.

# Capítulo 2

# Sistemas de numeração posicionais

## 2.1 Introdução

O que é o chamado "sistema decimal" ?

O que são os sistemas binário, octal, hexadecimal?

O que são os sistemas posicionais?

A Arte de Contar atinge seu ápice histórico, científico e social com os sistemas de numeração posicionais. O mais importante deles é o decimal, que pode ser considerado uma das maiores invenções da humanidade. Está hoje difundido em todo o planeta, e é utilizado nos mais diversos setores da organização social, assim como pela maior parte das aplicações científicas. Outro sistema posicional, o binário, assumiu grande importância nos dias atuais, pois tornou viável a implementação de uma linguagem para uso na computação digital.

## 2.2 Gênese dos sistemas posicionais

Os conceitos de posição e de agrupamento constituem a base da invenção dos sistemas posicionais. Que civilização e que pessoas teriam concebido essas ideias como recurso para a contagem? Talvez algum cientista que trabalhava em um antigo observatório astronômico, sustentado por um rei visionário, ou algum gênio enfurnado em sua biblioteca, procurando uma maneira mais avançada de representar os números naturais?

Provavelmente isso ocorreu de uma forma bem mais prosaica. Talvez essas ideias tenham aparecido em inúmeras situações para as mais diversas pessoas, ao pastor de ovelhas que precisava conferir seu rebanho ao fim de um dia de pastoreio, ao fiscal aduaneiro que precisava conferir os volumes das mercadorias descarregadas no porto, ao financista que precisava contar as moedas, ao encarregado do abastecimento de um exército. O fato é que as ideias de agrupamento e posição são relativamente simples, o mais complicado é transformar esse conhecimento em um sistema posicional completo, socialmente utilizável, com recursos de registro duráveis e pouco dispendiosos, e com o desenvolvimento de algoritmos compactos para implementação das operações aritméticas.

Se você fosse pastor e precisasse conferir a presença de 47 ovelhas no curral poderia simplesmente contá-las: uma, duas, três, etc. Mas, como pastor de ovelhas na antiga Pérsia ou outro

lugar qualquer daqueles tempos, você provavelmente seria analfabeto e não saberia os nomes de tantos números. Nessa situação uma forma de conferir a quantidade de ovelhas seria ter uma bolsa com 47 pedrinhas, e fazer a correspondência uma a uma entre as pedrinhas e as ovelhas. A partir dessa forma não seria difícil inventar outras possibilidades mais econômicas, usando uma quantidade bem menor de pedrinhas, como fazer a correspondência das ovelhas com os dedos de sua mão, e a cada dez ovelhas colocar uma pedra em um determinado lugar. A quantidade de ovelhas estaria correta com quatro pedras e sete dedos contados. Vemos que a unidade antes representada por uma pedrinha adquire uma qualidade adicional, a de representar um grupo de dez unidades. Dessa forma ilustramos o uso do conceito de agrupamento na contagem.

Em [54], página 117, o autor descreve que em Madagáscar, até há pouco tempo, o seguinte método era utilizado para conferir a quantidade de guerreiros. Fazia-se uma pilha de seixos, em número de um a dez, à medida que os guerreiros iam sendo contados. Quando a pilha perfazia dez seixos, eles eram recolhidos, e era colocado um seixo em uma segunda posição. Recomeçava-se a primeira pilha, contando de um a dez, quando então os seixos eram novamente recolhidos, e colocado um outro seixo na segunda pilha. E assim se prosseguia até a segunda pilha atingir dez seixos, que eram recolhidos, e uma terceira pilha tinha início. Portanto cada seixo da primeira pilha valia uma unidade, cada seixo da segunda pilha valia dez unidades, e cada seixo da terceira pilha, cem unidades. Fica claro que podemos prosseguir com quantas pilhas sejam necessárias, convencionando que um seixo de uma determinada pilha tem um valor dez vezes maior do que se ele estivesse na pilha que a antecede. Dessa forma ilustramos o uso do conceito de posição na contagem.

Vimos dois exemplos em que as ideias de posição e de agrupamento são utilizadas como recurso para sintetizar a representação de números. Entretanto isso não significa que seu uso permite uma passagem tranquila para o conceito pleno de sistema de numeração posicional. Basta observar que o ábaco adota os conceitos de agrupamento e de posição, e pode ser usado tanto para sistemas aditivos como para posicionais. Por isso mesmo o ábaco serviu de instrumento de transição entre os dois tipos de sistemas.

A construção de um sistema posicional com uso constante em ambientes sociais e científicos foi realizada no mundo antigo por apenas três povos: os sumérios, os maias e os hindus. Essa construção certamente exigiu a liderança de uma inteligência científica e uma decisão coletiva, ou pelo menos governamental, em adotar o sistema.

O método hindu foi o que trouxe resultados mais convenientes para nossa civilização. Primeiramente devido ao fato do sistema usar a base dez, uma escolha bastante prática e adequada, devido a que temos dez dedos nas mãos. Em segundo lugar porque os hindus se preocuparam em criar um sistema adaptado à escrita em papel. Embora não tenhamos registros históricos detalhados do trabalho dos hindus, podemos presumir que inicialmente utilizavam o ábaco para representar números, e criaram algoritmos para implementar as operações aritméticas nesse instrumento. O ábaco era, de fato, o método mais barato e disponível para a prática de qualquer aritmética. Entretanto, o ábaco tem um sério inconveniente, que é o de nada deixar registrado. Daí a necessidade de se criar um método de registro durável, e os hindus tiveram a feliz ideia de transpor sua aritmética do ábaco para a escrita em papel.

A construção de um sistema de numeração posicional decimal para registro em papel exige o reconhecimento de que devem ser usados exatamente dez símbolos, nove para representar os números de um a nove, e mais um símbolo para representar a casa vazia. Exige também a construção de convenções como decidir se a escrita dos valores das casas de um dado número será feita em linha, se essa linha é vertical ou horizontal, e de que lado da representação deve ficar o valor das unidades.

Terminamos esta seção observando que os soldados de um quartel podem ser contados de

uma forma mais sintética. Como eles são treinados para fazer formações, podem ser organizados grupos como esquadrões com cem componentes cada. É fácil conferir visualmente a quantidade de soldados em um esquadrão. Os restantes podem ser organizados em pelotões com dez em cada. Os que restam desses pelotões ficam separados. Dessa forma podemos contar os esquadrões, os pelotões e os soldados restantes, e conferir sua quantidade sem necessidade de contar um a um.

**Exemplo 2.1.** Um indivíduo faz a contagem dos votos de uma assembléia em uma pequena lousa, marcando cada voto com um traço de giz. A cada quatro votos desenha um quadrado, e os dois votos seguintes são marcados como suas diagonais. Depois de desenhar vários desses quadrados cruzados constatou que a lousa não tinha espaço suficiente, e resolveu representar com um círculo cada grupo de cinco deles. No final da votação a lousa ficou assim:

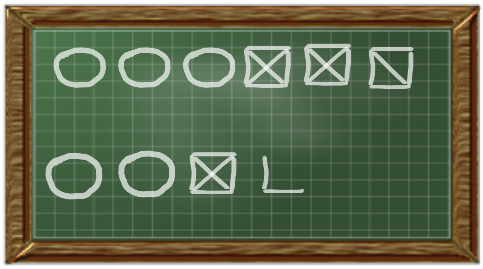


Figura 2.1. Na lousa estão representados os números

$$30 + 30 + 30 + 6 + 6 + 5 = 107 \text{ (linha de cima)}$$

e

$$30 + 30 + 6 + 2 = 68 \text{ (linha de baixo).}$$

Vemos que esse singelo método de numeração usa essencialmente três símbolos, o traço, o quadrado cruzado e o círculo. Está nele presente o conceito de agrupamento, já que organiza as unidades em grupos de seis e de trinta. Observe que não utiliza o recurso da posição: os símbolos podem ser trocados de lugar sem prejuízo do valor.

**Exemplo 2.2.** Retomando o Exemplo anterior, podemos representar algebricamente aquele sistema da seguinte forma. Indicando o círculo com a letra $C$, o quadrado cruzado com a letra $Q$ e a unidade com $U$, um número natural qualquer é da forma

$$aC + bQ + cU,$$

com as letras $a$, $b$ e $c$ representando números naturais, sendo que $c$ pode estar ausente ou é $\leq 5$, $b$ pode estar ausente ou é $\leq 4$ e $a$ pode estar ausente ou é um número natural qualquer. Exemplos:

$$2C + 3Q + 2U, \quad 4Q + 3U, \quad 17C, \quad 7C + 3U.$$

Essas representações podem ser sintetizadas por

$$(2;3;2)_{lousa}, \quad (0;4;3)_{lousa}, \quad (17;0;0)_{lousa}, \quad (7;0;3)_{lousa}.$$

Esse sistema necessita de um método auxiliar para escrever os números $a$, $b$ e $c$. Para isso estamos usando o sistema decimal. Vemos assim que esse sistema tem uso muito localizado, servindo apenas para certas situações práticas bastante limitadas. Mas é matematicamente válido, pois todo número tem um sucessor. Por exemplo, o sucessor de $3C + 4Q + 4U$ é $3C + 4Q + 5U$, e deste é $4C$. O sucessor de $aC + 4Q + 5U$ é $(a+1)C = (a+1;0;0)_{lousa}$.

## 2.3 Problemas

**Problema 2.3.1.** Suponha que em Madagáscar, conforme descrito no texto, foram contados, um a um, 456 guerreiros. Qual o número mínimo de seixos necessários para se efetuar essa contagem? Quantos esquadrões completos podem ser formados com essa quantidade de guerreiros? Quantos pelotões? O que significa 5 nessa situação?

**Problema 2.3.2.** Segundo relato de [30], página 22, um indivíduo contava o gado de uma fazenda da seguinte forma. A cada cinquenta bois abaixava um dedo (a pessoa sabia contar de um a cinquenta). A cada cinco dedos guardava uma pedrinha no bolso. **a)** Ao final de uma contagem o indivíduo tinha cinco pedrinhas no bolso, três dedos abaixados e restavam 27 bois extras contados. Quantos bois no total foram contados? **b)** Se a fazenda tem 1860 bois, depois que todos forem contados qual será a situação das pedrinhas, dedos e bois extras?

**Problema 2.3.3.** Descreva algebricamente o sucessor de qualquer número $aC+bQ+cU$ descrito no Exemplo 2.2.

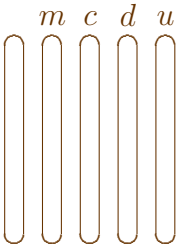
**Problema 2.3.4**. Um feirante utiliza uma balança de dois pratos e o seguinte conjunto de "pesos": um peso de 50 gr, um de 100 gramas, dois de 200 gramas, um de 500 gramas e 4 de 1 kg. (a) Se os pesos são colocados em apenas um prato, quais são os valores que podem ser medidos? (b) Se os pesos são colocados em qualquer prato, algum deles pode ser dispensado? Quais valores podem ser medidos? (c) Descreva algebricamente o sistema de representação nos dois casos. Esses sistemas são matematicamente corretos?



Figura 2.2. Balança de dois pratos.

## 2.4 O sistema posicional decimal

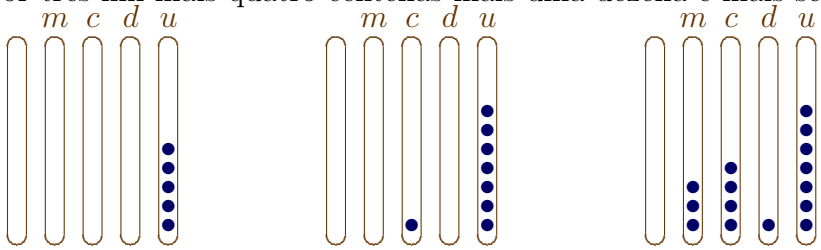
Iniciamos esta seção construindo o sistema posicional decimal para representação em um *ábaco*. Esse instrumento pode ser imaginado como uma placa de madeira com sulcos verticais, e uma coleção de pedrinhas. Cada um dos sulcos é denominado *casa*. As casas são numeradas da direita para a esquerda. A primeira casa é denominada *casa das unidades (u)*, a segunda, *casa das dezenas (d)*, a terceira, *casa das centenas (c)*, a quarta, *casa das unidades de milhares (m)*. As casas seguintes podem ser denominadas com a ordem de sua posição. Na figura vemos o desenho estilizado de um ábaco visto de cima.




Um ábaco com uma pedrinha colocada na casa das unidades representa o número um, com duas pedrinhas, o número dois, e assim por diante, com nove pedrinhas colocadas na casa das unidades representa o número nove. O número dez é representado no ábaco com uma pedrinha na casa das dezenas e nenhuma na casa das unidades. Podemos representar no ábaco qualquer número, desde que tenhamos uma quantidade suficiente de casas e de pedrinhas, usando as

seguintes regras: i) cada pedrinha colocada na primeira casa tem valor um; ii) cada pedrinha colocada na segunda casa ou nas seguintes tem valor dez vezes maior do que se estivesse colocada na casa imediatamente anterior; iii) numa casa qualquer a quantidade máxima de pedrinhas é nove, sendo que a casa pode estar vazia.

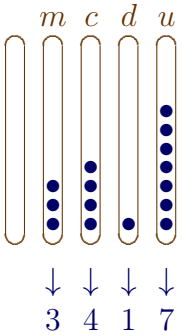
Na figura a seguir vemos três ábacos, cada um representando um número: o primeiro constituído por cinco unidades, o segundo por uma centena, nenhuma dezena e sete unidades, e o terceiro por três mil mais quatro centenas mais uma dezena e mais sete unidades.




Nosso próximo passo é construir uma forma de representar números no sistema posicional decimal de modo que eles possam ser escritos em uma folha de papel. A primeira providência que se faz necessária é desenhar símbolos para cada um dos números de um a nove. Já sabemos que esses símbolos são:

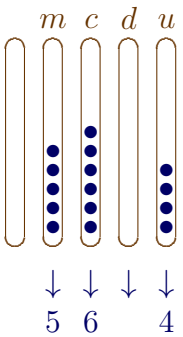
$$1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \quad 7 \quad 8 \quad 9$$

Tomamos como ponto de partida o dispositivo já construído para representar os números no ábaco. Os símbolos acima descrevem quantas pedrinhas existem em uma determinada casa. Imaginamos assim a seguinte transposição:




Portanto esse número é escrito em uma folha de papel simplesmente no formato 3417. Nessa representação dizemos que 7 ocupa a 1ª. casa, ou casa das unidades, 1 ocupa a 2ª. casa, ou casa das dezenas, etc.

Ao transpor a representação dos números do ábaco para o papel percebemos logo que temos um problema. O que fazer quando uma ou mais casas do ábaco estão vazias? Uma solução é nada escrever na casa ou casas correspondentes. Por exemplo,



e vemos que o número assim representado no ábaco, quando transposto para o papel, se escreve 56 4. Com essa notação podemos perceber que a primeira casa está ocupada por 4, representando quatro unidades, a segunda casa está vazia, 6 está na terceira casa representando seis centenas, e 5 está na quarta casa representando 5 milhares.

Mas a experiência logo nos indica que essa não é uma boa solução. Por exemplo, em 89 34 temos representados dois números diferentes, a saber, 89 e 34, ou será que se trata de um único número com duas casas vazias intermediárias, ou seriam três? Se observarmos que 34 pode ser simplesmente o número 34 ou 34 seguido de algumas casas vazias, então a confusão fica maior ainda. Uma solução para isso seria desenhar casas para os símbolos. As casas podem ser representadas por quadradinhos. Vemos abaixo um número com duas casas vazias intermediárias e uma casa vazia correspondente às unidades.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 7 | 9 | 5 | | | 3 | 9 | |

Já sabemos que a solução apresentada pelos hindus (e também pelos maias, sumérios e outros povos) foi muito melhor. Eles inventaram um símbolo exclusivo para indicar a casa vazia. Esse símbolo, que hoje denominamos *zero*, é indicado em nossos dias por 0. Usando essa ideia o número acima é representado por 79500390.

Temos agora todos os ingredientes necessários para definir o *sistema posicional decimal* usando uma simbologia algébrica adequada para representar os números na forma escrita. Segue a definição.

Consideramos os símbolos

$$0 \quad 1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \quad 7 \quad 8 \quad 9$$

que são chamados *algarismos decimais*. O símbolo 0 chama-se zero e os símbolos 1, 2, 3,..., 9 designam os números de um a nove, nessa ordem. Esses símbolos também são denominados *algarismos hindu-arábicos* devido à sua origem histórica.

Cada número natural é indicado por uma sequência de algarismos escritos em linha horizontal, um em seguida do outro, tendo como *regra do sucessor*:

*i)* se a representação de um número tem como unidade um dos algarismos 0, 1, ..., 8, então a representação do sucessor se obtém substituindo-se esse algarismo pelo seu sucessor na ordem natural dos algarismos;
*ii)* se a representação de um número tem como unidade o algarismo 9, então a representação do sucessor se obtém substituindo-se esse algarismo 9 por 0 e em seguida aplicando-se recorrentemente os itens *i)* e *ii)* dessa regra à casa seguinte. Se, ao aplicar essa recorrência, a casa seguinte não existir, considera-se como se ela tivesse o algarismo zero, que é, então, substituído por 1.

A forma geral de uma representação no sistema decimal é

$$d_n \dots d_2 d_1 d_0 \tag{2.1}$$

em que cada $d_i$ é um algarismo decimal, sendo $d_n \neq 0$, e $n = 0, 1, 2, \ldots$ Portanto os números naturais representados no sistema decimal são

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, \ldots, 19, 20, 21, \ldots, 98, 99, 100, 101, \ldots$$

Estivemos definindo o sistema decimal através da regra do sucessor. Sabendo representar o número 1 e sabendo representar o sucessor de qualquer número cuja representação esteja

dada, podemos representar todos os números naturais no sistema decimal. Com esse método representamos todos os números naturais contando-os um a um. Essa é a forma de contagem no sistema decimal que deriva diretamente da construção psicológica dos números naturais.

Existe outra maneira de obter a representação decimal de um número natural. Consiste em agrupar as unidades de um dado número em grupos de dez. Vejamos a que isso nos conduz.

Seja $m$ um número natural. Agrupamos as unidades de $m$ na maior quantidade possível de grupos de dez. Pode ocorrer nada sobrar ou pode restar 1 a 9 unidades. Seja $q_1$ a quantidade de grupos de dez assim formados e seja $d_0$ o que restou (portanto, $d_0$ é um algarismo de 0 a 9). Escrevemos $m = q_1 10 + d_0$. Tomamos $q_1$ e agrupamos as dezenas na maior quantidade possível de grupos de dez (portanto formamos grupos de 100 unidades). De novo pode ocorrer nada sobrar ou pode restar de 1 a 9 dezenas. Seja $q_2$ a quantidade de grupos de centenas e seja $d_1$ as dezenas que restaram. Escrevemos $q_1 = q_2 10 + d_1$. Note que $m > q_1 > q_2$. Prosseguindo, em algum passo encontramos um quociente $q_n$, que é a quantidade do maior agrupamento possível. Aqui paramos de agrupar. Note que $1 \leq q_n \leq 9$.

Resumimos esse procedimento com as seguintes relações algébricas:

$$\begin{aligned} m &= q_1 10 + d_0 \\ q_1 &= q_2 10 + d_1 \\ q_2 &= q_3 10 + d_2 \\ &\vdots \\ q_{n-1} &= q_n 10 + d_{n-1} \end{aligned}$$

Recompondo as relações acima e escrevendo $q_n = d_n$ vem

$$\begin{aligned} m &= q_1 10 + d_0 \\ &= (q_2 10 + d_1)10 + d_0 \\ &= q_2 10^2 + d_1 10 + d_0 \\ &\vdots \\ &= d_n 10^n + d_{n-1} 10^{n-1} + \cdots + d_1 10 + d_0 \end{aligned}$$

em que $d_i = 0, 1, 2, \ldots, 9$ para todo $i < n$ e $d_n = 1, 2, 3, \ldots, 9$ são algarismos decimais.

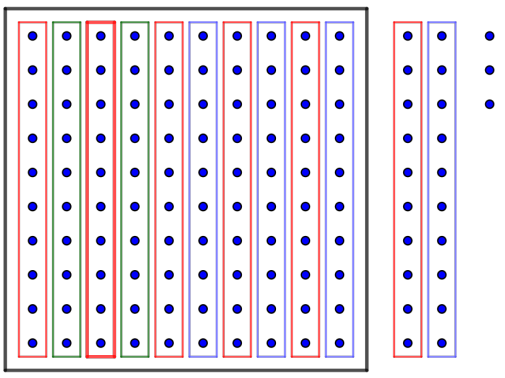


Figura 2.3. Construção da representação decimal 123 para contagem de cento e vinte e três bolinhas. Primeiramente reunimos as bolinhas em grupos de dez, e sobram três. Portanto o dígito das unidades na representação decimal é 3. Dos doze grupos de dez separamos um grupo com dez deles, e sobram dois. Portanto o dígito das dezenas é 2. O procedimento finaliza, pois os grupos de centenas não ultrapassam 9. O último dígito é 1. Logo a representação decimal é 123.

Temos, portanto, duas formas de representação de $m$:

$$d_n d_{n-1} \ldots d_2 d_1 d_0 \qquad \text{e} \qquad d_n 10^n + d_{n-1} 10^{n-1} + \cdots + d_1 10 + d_0.$$

A expressão $d_n d_{n-1} \ldots d_2 d_1 d_0$ chama-se *forma compacta da representação decimal de* $m$, ou simplesmente *representação decimal de* $m$. A expressão $d_n 10^n + d_{n-1} 10^{n-1} + \cdots + d_1 10 + d_0$

chama-se *forma expandida da representação decimal de* $m$. Para dirimir possíveis confusões a representação compacta pode vir escrita como $(d_n d_{n-1} \dots d_2 d_1 d_0)_{dez}$.

O sistema posicional decimal também pode ser chamado de *sistema de base dez*. Dizemos ainda que dez (ou 10) é a *base* desse sistema.

Dada uma representação $d_n d_{n-1} \dots d_2 d_1 d_0$, os valores $d_i$ chamam-se *dígitos decimais* do número, ou, simplesmente, *dígitos*, quando o contexto deixa claro que se trata de base dez.

A leitura de um número natural representado no sistema decimal pode ser feita nomeando-se seus dígitos um a um, da esquerda para a direita. Por exemplo, 408 739 se lê: quatro zero oito sete três nove.

A leitura de um número na língua portuguesa é explicada na seção 2.10.

Uma última observação. Obtivemos a representação decimal de um número natural qualquer de duas formas: pela regra do sucessor e por agrupamento. Resta saber se esses dois métodos fornecem a mesma representação para um dado número qualquer. Para ver que isso é verdade observe que a regra do sucessor também agrupa as unidades do número. Ao contar os números a partir de 1 usando a regra do sucessor, sempre que se atinge dez unidades numa determinada casa, a casa posterior aumenta de uma unidade, contando assim mais um agrupamento. E vice-versa, se uma casa é aumentada de uma unidade significa que se obteve mais um agrupamento correspondente àquela casa. Assim os dois métodos são equivalentes. Na verdade, qualquer que seja o método de obtenção da representação decimal, ela será sempre a mesma. Uma demonstração formal desse fato está feita no Capítulo 6.

**Problema resolvido 2.3.** Em um número com dois dígitos o valor das dezenas é o triplo do das unidades. Trocando-se os dois dígitos entre si se obtém um número que, somado com o primeiro, resulta 132. Qual é o primeiro número?

*Solução 1.* Por exame de todos os casos. Como o dígito das dezenas é o triplo do das unidades, ele só pode ser 1, 2 ou 3. De fato, o dígito das unidades não pode ser $\geq 4$, pois nesse caso o dígito das dezenas seria $\geq 12$ o que não é possível. Portanto o número só pode ser: 31, 62 ou 93.

Agora examinamos as somas:

$$31 + 13 = 44, \qquad 62 + 26 = 88, \qquad 93 + 39 = 132.$$

Portanto o número é 93.

*Solução 2.* Com uso de notação algébrica. Seja $(ab)_{dez}$ o número dado. As condições apresentadas nos dizem que $a = 3b$ e que $(ab)_{dez} + (ba)_{dez} = 132$.

Como $(ab)_{dez} = 10a + b$ e $(ba)_{dez} = 10b + a$, temos $10a + b + 10b + a = 132 \Rightarrow 11a + 11b = 132 \Rightarrow 11(a + b) = 132 \Rightarrow a + b = 12$. Substituindo $a$ por $3b$ vem $4b = 12$ ou $b = 3$. Assim $a = 3b = 9$ e o número é 93. □

Examinando as somas $32 + 23 = 44$, $62 + 26 = 88$ e $93 + 39 = 132$ feitas acima, percebemos que têm algo em comum: são múltiplos de 11 (um múltiplo de 11 é um produto da forma $11m$, sendo $m$ um número natural). Isso nos sugere o seguinte resultado:

**Problema resolvido 2.4.** O *reverso* do número natural $d_n \dots d_1 d_0$ é o número $d_0 d_1 \dots d_n$ (pode-se assumir que $d_0 \neq 0$). Mostre que a soma de um número de dois dígitos com seu reverso é sempre um múltiplo de 11.

*Solução.* Seja $(ab)_{dez}$ um número com dois dígitos. Seu reverso é $(ba)_{dez}$. Lembrando que $(ab)_{dez} = 10a + b$ e que $(ba)_{dez} = 10b + a$, sua soma pode ser escrita como

$$(ab)_{dez} + (ba)_{dez} = 10a + b + 10b + a = 11a + 11b = 11(a + b).$$

Portanto a soma de um número de dois dígitos com seu reverso é um múltiplo de 11. □

Observamos que esse problema também pode ser resolvido por exame de todos os casos. Basta considerar todos os números de 10 a 99 e fazer a conta com cada um deles ...

## 2.5 Problemas

**Problema 2.5.1.** Um ábaco decimal usa pedrinhas para representar a unidade. Qual o número mínimo de pedrinhas necessárias para representar no ábaco os números de 1 a 1200, um a um?

**Problema 2.5.2.** Descreva algebricamente o sistema de numeração utilizado pelo indivíduo que contava bois no Problema 2.3.2. Em outros termos, se $(abc)_{boi}$ é a representação de um número nesse sistema, descreva a representação expandida. Nessa fórmula o que são $a$, $b$ e $c$, e que valores podem assumir? Qual é o sucessor de $(a4(49))_{boi}$? Descreva a regra geral do sucessor. Esse é um sistema de numeração matematicamente significativo?

**Problema 2.5.3.** Uma criança, ao contar as bolas de uma cesta, se enganou, e começou com vinte. Prosseguiu com vinte e um, vinte e dois, contando corretamente daí por diante, a última bola foi contada como trinta e nove. Quantas bolas existem na cesta?

**Problema 2.5.4.** Começando de 1 e enumerando os números um a um até contar 1579, quantos foram contados? Por quê? Começando de 29 e enumerando os números um a um até contar 1579, quantos foram contados? Por quê?

**Problema 2.5.5.** Quantos são os números naturais de 1 a 1000 para os quais a soma dos dígitos é 5?

**Problema 2.5.6.** Descubra todos os números com as seguintes propriedades: ele tem dois dígitos, o dígito das dezenas é o dobro do das unidades, e trocando os dois dígitos entre si se obtém um número que subtraído do primeiro resulta 36. Resolva esse problema usando dois tipos de solução: por exame de todos os casos e por notação algébrica. Qual forma é mais fácil?

**Problema 2.5.7.** Se $a$ e $b$ são algarismos decimais tais que $a+b=7$, então $(aba)_{dez}$ é múltiplo de 7.

**Problema 2.5.8.** Um estudante, para saber se 203 é múltiplo de 7, fez a seguinte conta: $20-2\times 3=14$. Como 14 é múltiplo de 7, então 203 também é, concluiu ele. Generalize e obtenha uma justificativa algébrica. O método vale para qualquer número? Explique tudo.

**Problema 2.5.9.** Qual é o dígito da casa das unidades do número $n=10q+a$ em que $q$ é um número natural qualquer e $a$ é um algarismo? E quais são os dígitos das casas das unidades e das dezenas do número $m=100q+a$?

**Problema 2.5.10.** Justifique por que o quadrado de um número de dois dígitos terminado em 5 pode ser obtido da seguinte maneira: multiplique o dígito das dezenas do número dado pelo seu sucessor e escreva 25 à direita do resultado. Novamente resolva esse problema usando dois tipos de solução: por exame de todos os casos e por notação algébrica. Qual forma é mais fácil?

**Problema 2.5.11.** Justifique por que o quadrado de um número de três dígitos terminado em 5 pode ser obtido da seguinte maneira: multiplique o número formado pelos dígitos das centenas e das dezenas, nessa ordem, pelo seu sucessor e escreva 25 à direita do resultado. Qual é a forma é mais fácil de resolver esse problema: por exame de todos os casos ou por notação algébrica?

**Problema 2.5.12.** Investigue se é possível obter uma regra prática para o cálculo do quadrado de um número qualquer cujo dígito das unidades seja 5. Não se esqueça de justificar.

**Problema 2.5.13.** Considere um número $m = d_n \dots d_2 d_1 d_0$ representado na forma geral (2.1). Diga o que representam, em relação às unidades de $m$, cada um dos valores: **a)** $d_0$; **b)** $d_1$; **c)** $d_2$; **d)** $d_n \dots d_2 d_1$. **e)** Indique a quantidade de centenas que podemos formar com as unidades de $m$.

**Problema 2.5.14.** Em uma escola as salas de aula estão identificadas por números de dois dígitos. Um estudante observa nos números consecutivos de quatro salas que a soma dos dígitos das dezenas coincide com a soma dos dígitos das unidades. Quais são os números?

**Problema 2.5.15.** Em uma estrada um marco de quilometragem traz um número com dois dígitos. A uma certa distância $d$ adiante um marco traz um número com os mesmos dígitos do marco anterior mas em casas trocadas. Mais adiante, num terceiro marco, situado à distância $d$ do segundo, novamente aparecem os mesmos dígitos, na mesma ordem que no primeiro marco, mas com um zero na casa do meio. Ache os números e a distância $d$.

**Problema 2.5.16.** Olhe bem para esse símbolo: **125**

Procure distinguir qual foi a ideia que primeiro lhe veio à mente ao ver o símbolo 125. Depois de descrever isso, procure perceber outras ideias associadas ao símbolo 125.

**Problema 2.5.17.** Quantos são os números naturais de três dígitos em cuja representação não comparecem os algarismos 2, 5, 7 ou 8?

**Problema 2.5.18.** Reveja o Problema Resolvido 2.4 e mostre agora que a soma de um número de quatro dígitos com seu reverso é sempre um múltiplo de 11. Isso acontece também para números com três dígitos?

**Problema 2.5.19.** Um número natural chama-se *palíndromo* ou *capicua* quando sua representação decimal for igual à sua representação reversa. Demonstre que todo número capicua com dois dígitos é múltiplo de 11. E quanto a números com três ou quatro dígitos?

**Problema 2.5.20.** Um número natural diz-se *automórfico* quando reaparece no final da representação decimal de seu quadrado. Os números automórficos de um dígito são 1, 5 e 6, e também o algarismo zero, se o considerarmos um número. Um número automórfico de dois dígitos é 25, pois $25^2 = 625$. Determine todos os números automórficos de dois dígitos.

## 2.6 Sistemas posicionais em uma base qualquer

Todo número natural $\beta \neq 1$ pode servir de base para a construção de um sistema posicional, o que pode ser feito de forma análoga à do sistema decimal. O método de representação assim obtido é denominado *sistema posicional de base* $\beta$, ou simplesmente *sistema de base* $\beta$, quando estiver claro no contexto que se trata de um sistema posicional. Dizemos ainda que $\beta$ é a *base* desse sistema.

Dado um número natural $\beta \neq 1$, escolhemos $\beta$ símbolos, um para indicar a casa vazia, e $\beta - 1$ para indicar os números de 1 a $\beta - 1$. Esses símbolos são chamados *$\beta$-algarismos*. Convencionamos que a casa vazia será sempre indicada por 0 (zero) e a unidade por 1.

A representação dos números naturais no sistema posicional de base $\beta$ segue as mesmas convenções do sistema decimal, adaptando-se a regra do sucessor conforme segue:

*i)* se a representação de um número tem como unidade um dos algarismos que representam 0, 1, ..., $\beta-2$, então a representação do sucessor se obtém substituindo-se esse algarismo pelo seu sucessor na ordem natural dos algarismos. $\beta-2$ é o antecessor de $\beta-1$.
*ii)* se a representação de um número tem como unidade o algarismo que representa $\beta-1$, então a representação do sucessor se obtém substituindo-se esse algarismo por zero e em seguida aplicando-se recorrentemente os itens *i)* e *ii)* dessa regra à casa seguinte. Se a casa seguinte não existir considera-se como se ela tivesse o valor zero, que é então substituído por 1.

Dado um número natural $m$, podemos obter sua representação na base $\beta$ através da regra do sucessor ou agrupando as unidades de $m$ em grupos de $\beta$. Assim, de modo inteiramente análogo ao que fizemos para o sistema decimal, vemos que $m$ tem duas formas de representação, a compacta e a expandida:

$$m = d_n d_{n-1} \dots d_2 d_1 d_0 = d_n\beta^n + d_{n-1}\beta^{n-1} + \dots + d_1\beta + d_0 \tag{2.2}$$

em que cada $d_i$ é um $\beta$-algarismo e $d_n \geq 1$.

Quando é necessário esclarecer em que base o número está sendo representado usamos a notação $(d_n d_{n-1} \dots d_2 d_1 d_0)_\beta$. Dada uma representação $d_n d_{n-1} \dots d_2 d_1 d_0$ em um sistema de base $\beta$, os valores $d_i$ se chamam *$\beta$-dígitos* do número, ou simplesmente *dígitos* se no contexto estiver claro de que base se trata. Se $\beta = 2$ os valores $d_i$ se chamam também *dígitos binários*. Na lingua inglesa se escreve *binary digit*, do que procede a abreviatura *bit*, muito usada na Ciência da Computação.

Consideremos um exemplo tomando quatro como base. Para construir o sistema de numeração posicional de base quatro precisamos primeiro escolher quatro símbolos, três para os números de um a três e um para designar a casa vazia. Por facilidade escolhemos os símbolos conhecidos

0 1 2 3

com os mesmos nomes pelos quais são denominados normalmente: zero, um, dois, três. Esses serão os algarismos de nosso sistema de base quatro.

Começamos contando: 1, 2, 3. E quem é o sucessor de 3 na base quatro? Observe que já contamos todos os números com um dígito. O sucessor é o menor número com dois dígitos. Usando a regra do sucessor na base quatro vemos que o dígito 3 deve ser substituído por 0 e a casa anterior deve ser ocupada por 1. Portanto o sucessor é 10 (lê-se *um zero*). E assim por diante, a contagem na base quatro é:

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 10 | 11 | 12 | 13 | 20 | 21 | 22 | 23 | 30 | 31 | 32 | 33 |
| 100 | 101 | 102 | 103 | 110 | 111 | 112 | 113 | 120 | 121 | 122 | 123 | 130 | 131 | 132 | 133 |
| 200 | 201 | 202 | 203 | 210 | 211 | 212 | 213 | 220 | 221 | 222 | 223 | 230 | 231 | 232 | 233 |
| 300 | 301 | 302 | 303 | 310 | 311 | 312 | 313 | 320 | 321 | 322 | 323 | 330 | 331 | 332 | 333 |

e o número seguinte é 1000 (lê-se *um zero zero zero*).

A representação de números na base quatro (ou em outra base qualquer) precisa de uma notação de modo que não haja confusão com a base dez sempre que usarmos para algarismos os mesmos símbolos. Assim, conforme já observamos, o número 1000 da base quatro, por exemplo, pode ser representado por $(1000)_{quatro}$ se o contexto der margem a alguma dúvida. Podemos também usar $(1000)_4$ mas isso não é tão bom, pois o símbolo 4 não existe na base quatro. Lembremo-nos também de chamar $(1000)_{quatro}$ de *um zero zero zero* e não de *mil*, pois $(1000)_{quatro}$ não é mil.

As bases posicionais mais comuns nas aplicações científicas são as de dois até dezesseis. A base sessenta é de interesse histórico, pois foi adotada pelos sumérios, assim como a base vinte,

escolhida pelos maias. Dentre esses os sistemas posicionais mais usados são: binário (dois), ternário (três), quaternário (quatro), quinário (cinco), octenário ou octal (oito), nonário (nove), decimal (dez), undecimal (onze), duodecimal (doze) e hexadecimal (dezesseis). O binário é o sistema natural das máquinas digitais, mas são usados também pela Ciência da Computação os sistemas quaternário, octal e hexadecimal.

Costuma-se escolher como algarismos para as bases de dois a dez os símbolos correspondentes utilizados no sistema decimal. Para as bases maiores costuma-se considerar, a partir de 9, a sequência de letras do alfabeto na forma capital: $A$, $B$, $C$, etc.

Por exemplo, para o sistema duodecimal os algarismos comumente adotados são:

$$0 \quad 1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \quad 7 \quad 8 \quad 9 \quad A \quad B$$

Vejamos como fica a contagem no sistema duodecimal:

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B |
| 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 1A | 1B |
| 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 2A | 2B |

e assim por diante, o maior número com duas casas é $(BB)_{doze}$, e seu sucessor é $(100)_{doze}$.

Para o sistema sexagesimal (base sessenta), de interesse histórico, teríamos que construir sessenta símbolos diferentes, e aqui nem a letras de nosso alfabeto seriam suficientes. Uma forma é adotar os nossos próprios números de zero a cinquenta e nove, e, na representação dos números, separar as casas com vírgula para evitar confusão. Assim o número sexagesimal

$$(21, 35, 47, 58)_{sessenta}$$

tem quatro casas, sendo 58 unidades, 47 grupos de sessenta, 35 grupos de sessenta vezes sessenta e 21 grupos de sessenta vezes sessenta vezes sessenta. No nosso sistema decimal esse número é

$$(21, 35, 47, 58)_{sessenta} = 21 \times 60^3 + 35 \times 60^2 + 47 \times 60 + 58 = 4\,664\,878.$$

Outra forma de construir algarismos sexagesimais seria unir graficamente cada dois símbolos decimais para formar um único símbolo. Por exemplo, o número dado acima seria representado por

$$\text{21}\,\text{35}\,\text{47}\,\text{58}$$

em que fica claro quais são os dígitos de cada casa. Uma terceira forma, sugerida em [45], página 74, consiste em convencionar que os algarismos sexagesimais são indicados sempre por dois dígitos decimais, acrescentando o algarismo zero à esquerda se for necessário. Dessa forma podemos omitir qualquer outra notação, pois fica claro quais são as casas. Por exemplo, $(19, 6, 35, 8)_{sessenta}$ pode ser representado por $(19063508)_{sessenta}$.

É fácil transpor um número de uma base para outra, conforme veremos.

Para transpor um número de outra base para a base dez basta expandir a representação e implementar os cálculos na base dez. Exemplos:

$$(11011)_{dois} = 1 \times 2^4 + 1 \times 2^3 + 0 \times 2^2 + 1 \times 2 + 1 = 27,$$

$$(3605)_{sete} = 3 \times 7^3 + 6 \times 7^2 + 0 \times 7 + 5 = 1328,$$

$$(A0B)_{doze} = A \times 12^2 + 0 \times 12 + B = 10 \times 12^2 + 0 \times 12 + 11 = 1451.$$

Para transpor da base dez para outra base $\beta \neq 10$ podemos utilizar a técnica do agrupamento. Dado um número na base dez, agrupamos suas unidades em grupos de $\beta$. O valor que sobra é um $\beta$-algarismo, e ele é o dígito das unidades do número na base $\beta$. E assim por diante.

Como exemplo transpomos 127 para a base três. Quantos grupos de três podemos fazer com 127 elementos? Calculamos

$$127 = 3 \times 42 + 1.$$

Com isso já sabemos que o dígito das unidades da representação de 127 na base três é 1. Assim $127 = (???1)_{três}$. Para calcular o dígito seguinte vemos quantos grupos de três podemos fazer com 42. Temos $42 = 3 \times 14 + 0$, e assim $127 = (??01)_{três}$. Agora $14 = 3 \times 4 + 2$, de modo que $127 = (??201)_{três}$. Como $4 = 3 \times 1 + 1$, temos $127 = (?1201)_{três}$. O último quociente é 1, que é menor do que três, portanto ele é o último dígito. Dessa forma

$$127 = (11201)_{três}.$$

Conferindo:

$$(11201)_{três} = 1 \times 3^4 + 1 \times 3^3 + 2 \times 3^2 + 0 \times 3 + 1 = 127.$$

Para transpor de uma base não decimal para outra não decimal podemos usar a base dez como passagem intermediária. Vejamos um exemplo. Vamos transpor $(6035)_{sete}$ para a base cinco. Primeiro transpomos $(6035)_{sete}$ para a base dez. Temos

$$(6035)_{sete} = 6 \times 7^3 + 0 \times 7^2 + 3 \times 7 + 5 = 2084.$$

Agora transpomos 2084 para a base cinco. Temos

$$\begin{aligned} 2084 &= 416 \times 5 + 4, \\ 416 &= 83 \times 5 + 1, \\ 83 &= 16 \times 5 + 3, \\ 16 &= 3 \times 5 + 1, \\ 3 &= 0 \times 5 + 3. \end{aligned}$$

Portanto $2084 = (31314)_{cinco}$. Em resumo,

$$(6035)_{sete} = 2084 = (31314)_{cinco}.$$

Existe uma forma de transpor de uma base não decimal para outra não decimal sem usar a base dez como intermediária. Explicaremos com fazer isso na Subseção 3.6.2.

Já observamos que o binário é o sistema natural das máquinas digitais, mas são usados também pela Ciência da Computação os sistemas quaternário, o octal e o hexadecimal. Esses sistemas guardam uma correspondência natural entre si, de modo que é fácil transpor um número de um para o outro. A conversão entre essas representações pode ser feita através de tabelas, facilitando a construção de algoritmos rápidos para a transposição de uma base para outra. Vejamos a tabela de transposição entre as bases binária e octal. O estudante pode conferir os valores.

| **Número binário** | **Algarismo octal** |
|---|---|
| 000 | 0 |
| 001 | 1 |
| 010 | 2 |
| 011 | 3 |
| 100 | 4 |
| 101 | 5 |
| 110 | 6 |
| 111 | 7 |

Para converter uma representação octal para binária basta usar diretamente a tabela, substituindo cada dígito octal pelos três dígitos binários correspondentes. Exemplo:

$$(57023)_{oito} = (101\,111\,000\,010\,011)_{dois}.$$

Se a última casa (contando da direita para a esquerda) da representação binária for ocupada por 0, eliminamos essa casa, o mesmo para a penúltima.

Para converter uma representação binária para octal separamos os dígitos do número binário dado em grupos de três, contando da direita para a esquerda, e se necessário acrescentamos à esquerda um ou dois algarismos 0 para que todos os grupos fiquem completos. Em seguida fazemos a conversão usando a tabela. Exemplo:

$$(1\,110\,100\,100\,101\,011\,110\,100)_{dois} =$$

$$= (001\,110\,100\,100\,101\,011\,110\,100)_{dois} = (16445364)_{oito}.$$

No Problema 2.7.11 o estudante é convidado a explicar algebricamente por que funciona essa tabela.

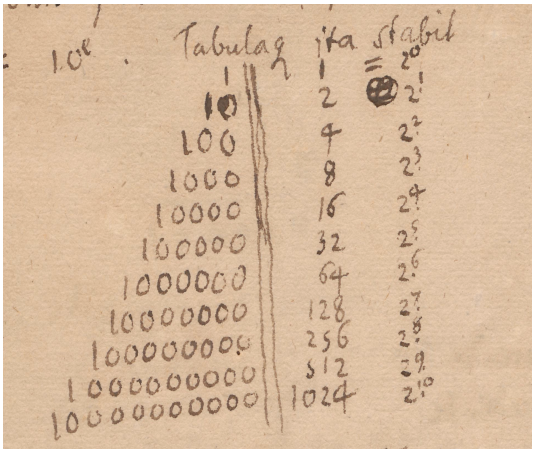



Figura 2.4. Digitalização de parte de manuscrito de Gottfried W. Leibniz com anotações sobre o sistema binário. Esse matemático fez estudos sobre esse sistema, de certo modo antecipando seu uso na moderna Ciência da Computação.

Podemos construir sistemas numéricos das mais variadas formas. Um exemplo significativo é a *expansão de Cantor*, ou *representação fatorial*. Um número natural $n$ qualquer é dado por

$$n = a_m m! + a_{m-1}(m-1)! + \ldots + a_2 2! + a_1 = (a_m; a_{m-1}; \ldots; a_2; a_1)_!$$

em que cada $a_i$ é um número natural $a_i = 0,\ 1,\ 2,\ \ldots,\ i$. A notação $m!$ chama-se *fatorial* de $m$ e significa o produto dos números de 1 a $m$, isto é, $m! = 1 \cdot 2 \cdot 3 \cdots (m-1) \cdot m$.

Para encontrar a representação fatorial de 500 observamos que 500 está entre 5! e 6! Dividindo 500 por 5! temos $500 = 4\times 5! + 20$. Por sua vez 20 está entre 3! e 4!, e temos $20 = 3\times 3! + 2$. Como $2 = 2!$ temos

$$500 = 4 \times 5! + 3 \times 3! + 1 \times 2! =$$

$$= 4 \times 5! + 0 \times 4! + 3 \times 3! + 1 \times 2! + 0 = (4; 0; 3; 1; 0)_!$$

Observe que a representação fatorial usa a sequência infinita 1!, 2!, 3!, ..., que tem um papel similar à da sequência 1, 10, $10^2$, ... no sistema decimal. Na representação fatorial todos os números naturais são algarismos, por isso necessitamos representá-los em um sistema auxiliar. Aqui usamos o decimal, mas poderia ser outro, como o sistema hexadecimal. Uma característica da expansão de Cantor é que ela permite uma representação mais compacta dos números, economizando memória nos computadores digitais.

**Problema resolvido 2.5.** Justifique por que se $a$ é um número natural cuja representação decimal tem $n$ dígitos, então $10^{n-1} \leq a < 10^n$. O que ocorre em sistemas de base $\beta$ qualquer?

*Solução.* Se $a$ tem um dígito, então $1 \leq a < 10$, ou seja, $10^{1-1} \leq a < 10^1$. Se $a$ tem dois dígitos, então $10 \leq a < 100$, ou seja, $10^{2-1} \leq a < 10^2$. Em geral, o menor número com $n$ dígitos é $100\ldots0$ com $n-1$ zeros, o que é o mesmo que $10^{n-1}$. Assim se $a$ tem $n$ dígitos então $10^{n-1} \leq a$. Por outro lado, como $10^n$ tem $n+1$ dígitos, segue que $a < 10^n$.

De forma análoga vemos que se $a$ é um número natural cuja representação no sistema de base $\beta$ tem $n$ dígitos, então $\beta^{n-1} \leq a < \beta^n$.

Vejamos outra forma de obter essa relação. Seja

$$m = d_{n-1}\beta^{n-1} + \cdots + d_1\beta + d_0$$

um número com $n$ dígitos na base $\beta$. Lembremos que $0 \leq d_i \leq \beta - 1$ para todo $i$ e que $1 \leq d_{n-1}$. Assim

$$m = d_{n-1}\beta^{n-1} + \cdots + d_1\beta + d_0 \geq d_{n-1}\beta^{n-1} \geq \beta^{n-1}.$$

Por outro lado,

$$m = d_{n-1}\beta^{n-1} + d_{n-2}\beta^{n-2} + \cdots + d_1\beta + d_0 \leq$$

$$\leq (\beta-1)\beta^{n-1} + (\beta-1)\beta^{n-2} + \cdots + (\beta-1)\beta + (\beta-1) =$$

$$= (\beta-1)\left[\beta^{n-1} + \beta^{n-2} + \cdots + \beta + 1\right] = (\beta-1)\frac{\beta^n - 1}{\beta - 1} = \beta^n - 1 < \beta^n.$$

Você notou que usamos a fórmula da soma dos termos de uma progressão geométrica. □

**Problema resolvido 2.6.** Quantos dígitos decimais e binários tem o primo de Mersenne $M = 2^{11213} - 1$, descoberto por Donald B. Gillies em 1963?

*Solução.* Nesse problema supomos que o estudante já estudou logaritmos. Calculemos primeiro a quantidade $n$ de dígitos decimais de $2^{11213}$. Do problema anterior temos

$$10^{n-1} \leq 2^{11213} < 10^n \Rightarrow \log 10^{n-1} \leq \log 2^{11213} < \log 10^n \Rightarrow$$

$$\Rightarrow n - 1 \leq 11213 \log 2 < n \Rightarrow n - 1 \leq 3375,449\ldots < n \Rightarrow n = 3376.$$

Note que não podemos ter $2^{11213} = 10^{n-1}$, pois isso implicaria $n - 1 = 11213 \log 2$, mas $11213 \log 2 \approx 3375,449$ não é um número natural. Portanto $2^{11213}$ não é o menor número

natural com $n$ dígitos decimais, e assim, $M = 2^{11213} - 1$ também tem $n$ dígitos, ou seja, 3376 dígitos decimais.

Vejamos agora a quantidade de dígitos binários. O número $2^{11213} = (100\ldots0)_{dois}$ tem 11213 zeros, portanto tem 11214 dígitos. Como esse é o menor número com 11214 dígitos binários, o número $M = 2^{11213} - 1$ tem 11213 dígitos binários. □

## 2.7 Problemas

**Problema 2.7.1.** Explique por que não pode haver sistema de numeração posicional de base um.

**Problema 2.7.2.** Um jovem afirmou que completou 100000 anos na data 100/1000/10000. Será ele de alguma civilização extra-terreste em que um mês tem mais do que 100 dias e o ano tem mais do que 1000 meses?

**Problema 2.7.3.** Temos aqui uma fileira de moedas. Conte-as na base quatro.



Qual é o número de moedas?

**Problema 2.7.4.** Você sabe contar em outras bases que não a base dez? Encontre o sucessor de cada um dos números abaixo usando a regra do sucessor da base indicada:

$$(78)_{nove} \quad (65)_{sete} \quad (16)_{sete} \quad (1011)_{dois} \quad (53AF)_{dezesseis}$$

**Problema 2.7.5.** Escreva os números de 1 a $(200)_{cinco}$ no sistema quinário. Faça o mesmo no sistema duodecimal de 1 a $(100)_{doze}$.

**Problema 2.7.6.** Um feirante, em certo dia, vendeu onze grosas e dez dúzias de ovos. Escreva esse número na base doze.

**Problema 2.7.7.** Quantas vezes cada um dos $\beta$-algarismos 0, 1, 2, ... aparece ao escrevermos os números de 1 a $(100)_\beta$ inclusive?

**Problema 2.7.8.** Responda e justifique usando apenas a base três: **a)** qual é o menor número com $(12)_{tres}$ dígitos? **b)** qual é o maior? **c)** quantos números existem com $(12)_{tres}$ dígitos?

**Problema 2.7.9.** No sistema de base $\beta$, qual é o menor número com $n$ dígitos? Qual é o maior? Quantos números existem com $n$ dígitos?

**Problema 2.7.10.** Transporte: **a)** $(21022)_{três}$ para o sistema decimal; **b)** 6477 para o sistema hexadecimal; **c)** 3107 para o sistema duodecimal; **d)** $(2A0B3)_{doze}$ para o sistema binário.

**Problema 2.7.11.** Explique algebricamente por que funciona a tabela de conversão entre as representações binária e octal, apresentada na página 33.

**Problema 2.7.12.** Construa uma tabela de conversão entre os sistemas binário e hexadecimal. Explique como se converte uma representação para outra, com justificativas. Usando essa tabela transponha $(1001101011100)_{dois}$ para o sistema hexadecimal. Transporte $(5F60AD)_{dezesseis}$ para o sistema binário. Essa ideia pode ser usada para outros conjuntos de sistemas?

**Problema 2.7.13.** A Ciência da Computação utiliza uma lista de dois algarismos hexadecimais para representar caracteres e sinais de texto. Essa lista vai de 00 até FF. Essas representações constituem a chamada tabela ASCII. Calcule (na base dez e na base dezesseis) quantas representações podem ser obtidas dessa forma.

**Problema 2.7.14.** A Ciência da Computação utiliza uma lista de seis algarismos hexadecimais para representar cores. Essa lista vai de 000000, que representa a cor preta, até FFFFFF, que representa a cor branca. Outras cores têm representações intermediárias. Calcule (na base dez e na base dezesseis) quantas cores podem ser representadas dessa forma.

**Problema 2.7.15.** Um estudante sugeriu o seguinte método para encontrar a representação decimal de $(35)_{doze}$. Como na base doze existem dois algarismos a mais que na base dez, calculamos $3 \times 2 = 6$, e $35 + 6 = 41$. Portanto, concluiu o estudante, $(35)_{doze} = 41$. Para obter a representação decimal de $(25)_{seis}$, ele fez $2 \times 4 = 8$, e $25 - 8 = 17$, portanto $(25)_{seis} = 17$. Confira, explique e verifique se o método funciona sempre.

**Problema 2.7.16.** Decida sobre uma convenção para os algarismos da base cem. Transponha 12 709 483 705 para a base cem.

**Problema 2.7.17.** Encontre a representação binária dos números de Fermat $2^{2^s} + 1$, $s = 0$, 1, 2, 3, ... Quanto à forma de calcular $2^{2^s}$, consulte nossa convenção na página 84.

**Problema 2.7.18.** Iniciando de 1, conte no sistema fatorial uma quantidade de números suficiente para você perceber a regra do sucessor e descrevê-la.

**Problema 2.7.19.** Na base dez, um número natural é par se o dígito das unidades for par, e ímpar se o dígito das unidades for ímpar. Como fica essa afirmação em outros sistemas de numeração posicionais? Como fica, em particular, para a base três?

## 2.8 Sistemas de numeração posicionais históricos

A concepção teórica e a difusão social de um sistema de numeração são mais complexas para os sistemas posicionais do que para os aditivos. Por isso ficamos admirados quando lemos que a civilização suméria desenvolveu um sistema posicional no terceiro milênio a.C. e o utilizava em suas escolas. Percebemos também que devido à heterogeneidade das raças e às dificuldades de registro e comunicação, civilizações posteriores, como a dos gregos e a dos romanos, se contentaram com sistemas aditivos, por opção ou por desconhecerem os sistemas posicionais.

Os sistemas posicionais registrados nos livros de história são o sistema sexagesimal dos sumérios, o sistema vigesimal dos maias e o sistema decimal dos hindus.

### O sistema sexagesimal sumério

A surpreendente civilização suméria se desenvolveu na Mesopotâmia a partir do quarto milênio a.C. Utilizava um sistema posicional de base sessenta, que permitiu certa facilidade em realizar cálculos aritméticos e em investigar propriedades dos números.

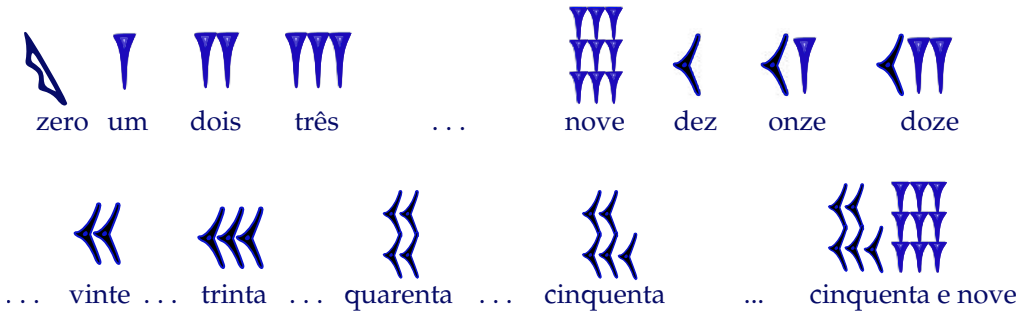
A técnica de escrita dos sumérios consistia em imprimir símbolos em tábulas de barro usando estilos com pontas de formatos variados. Uma dessas formas era a cunha, e por isso os caracteres sumérios são denominados *cuneiformes* (em forma de cunha). Diferentes caracteres

eram obtidos variando-se a inclinação do estilo. As tábulas eram depois cozidas até endurecer, constituindo um registro durável.

Esse método acarretava uma séria limitação, pois os símbolos assim disponíveis eram reduzidos. Para seu sistema de numeração os sumérios reservaram apenas dois caracteres, que representavam os números 1 e 10. Posteriormente introduziram um símbolo para o zero. Os desenhos mais usados hoje em dia para esses símbolos são:




Para aplicar o sistema posicional de base sessenta os sumérios necessitavam de símbolos para os algarismos de zero a 59. Com apenas três caracteres à disposição, escreviam esses algarismos através de um sistema aditivo, de acordo com a seguinte lista:




Usando esses algarismos os números naturais eram representados no método posicional. Exemplos:

$2 \times 60^2 + 3 \times 60 + 33$



$5 \times 60^3 + 0 \times 60^2 + 2 \times 60 + 0$



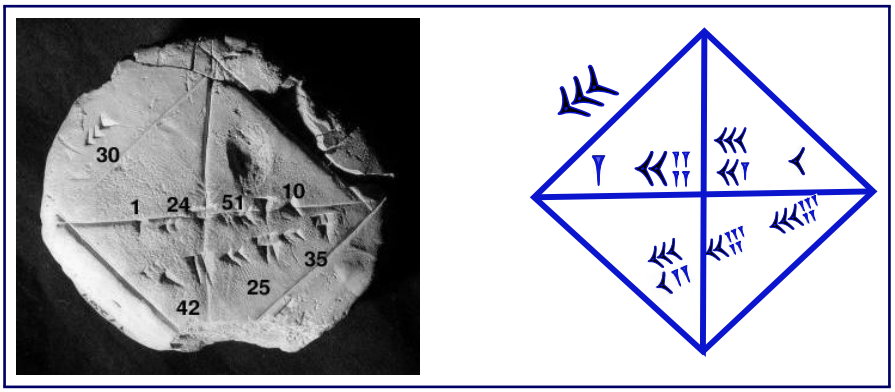



Figura 2.5. Tablete sumério mostrando numerais babilônicos, encontrado na Mesopotâmia e datado de 1800-1600 a.C. Exposto na *Yale Babylonian Collection's Tablet YBC 7289*. Fotografia de Bill Casselman. Sobre a licença para uso da imagem veja mais detalhes na página 260. Ao lado, desenho estilizado do tablete. Sobre o significado dos números nesse tablete confira [94], página 39 e seguintes.

De acordo com notação proposta em [84] e já comentada na página 32, podemos utilizar uma forma compacta para a base sexagesimal, como nos exemplos

$$27 \times 60^2 + 3 \times 60 + 33 = (27, 3, 33)_{sessenta} \quad \text{e}$$

$$53 \times 60^3 + 0 \times 60^2 + 2 \times 60 + 19 = (53, 0, 2, 19)_{sessenta}.$$

Os sumérios às vezes simplificavam a escrita de números pequenos usando um símbolo subtrativo. Observamos também que o caractere que representava o zero foi utilizado a partir de 300 a.C., mesmo assim muitas vezes era escrito apenas quando estava posicionado entre outros caracteres, sendo omitido quando deveria aparecer no final da representação. Antes da implementação do símbolo para o zero as casas vazias de uma determinada representação tinham que ser percebidas pelo contexto.

## O sistema numérico maia

A surpreendente civilização Maia, de origem desconhecida, deixou-nos inúmeros registros de sua ciência. Sua escrita numérica utilizava um sistema posicional baseado na sequência 1, 20, $18 \cdot 20$, $18 \cdot 20^2$, ...

Os glifos maias usados para representar os algarismos estão dispostos na tabela abaixo:

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| zero |  | 5 |  | 10 |  | 15 |  |
| 1 |  | 6 |  | 11 |  | 16 |  |
| 2 |  | 7 |  | 12 |  | 17 |  |
| 3 |  | 8 |  | 13 |  | 18 |  |
| 4 |  | 9 |  | 14 |  | 19 |  |

Os maias escreviam os números dispondo os dígitos verticalmente em uma coluna, com o dígito de maior valor colocado na parte de cima. Vejamos um exemplo:

$$19 \times 18 \cdot 20 + 0 \times 20 + 13 \quad \text{}$$

Os maias subdividiam o ano em 18 meses de 20 dias cada, perfazendo 360 dias. Acrescentavam 5 dias dedicados ao lazer e ao culto. Talvez isso explique por que utilizavam um sistema posicional misto com bases 20 e 18.

## 2.9 Pequena história do sistema de numeração decimal

Os hindus desenvolveram, nos primeiros séculos da nossa era, um sistema posicional decimal. Os historiadores não têm clareza se foi uma invenção independente ou se teve influências externas. O que se sabe com certeza é que no Século IV já utilizavam a notação posicional,

mas sem um símbolo para o zero. A mais antiga e conhecida ocorrência de um símbolo para o zero entre os hindus se encontra em uma inscrição do ano de 876. Mas seu uso pode ser ainda mais antigo conforme informação que consta na Figura 2.6.

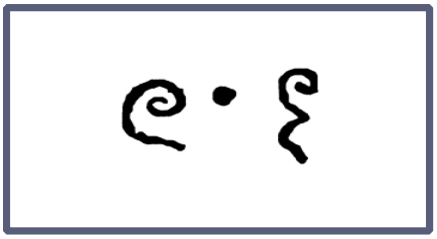


Figura 2.6. Desenho cotado de antiga inscrição localizada nas ruínas de um templo em Angkor, atual Camboja, e datada do ano de 683. Mostra o numeral 605 em caracteres khmer, que por sua vez são derivados de caracteres hindus. É o mais antigo registro conhecido do uso de um símbolo para o zero em um sistema de numeração posicional decimal.

Com a expansão da civilização árabe, seus estudiosos entraram em contato com o sistema de numeração decimal praticado pelos hindus. No Século VIII traduziram uma obra hindu contendo tabelas astronômicas. Os estudiosos árabes da escola de Bagdá tomaram contato com esse sistema, e reconheceram seu valor. Em 825 aproximadamente o matemático de origem persa al-Khowarizmi descreveu o sistema hindu de maneira completa em um pequeno livro.

A presença política e econômica dos árabes na Europa propiciou o aparecimento do sistema hindu entre os estudiosos latinos. Por volta de 980 esse sistema era estudado na Espanha. O livro de al-Khowarizmi foi traduzido para o latim aproximadamente em 1120, talvez por Adelardo de Bath, recebendo o nome de *Liber algorismi de numero hindorum*. Estudiosos europeus de vários países e das mais diversas áreas do conhecimento perceberam as vantagens do sistema posicional decimal em relação ao sistema romano vigente. Apesar disso o sistema decimal levou mais de quatro séculos para substituir o sistema romano, pois houve uma grande oposição de várias correntes de pensamento. Um dos autores que mais contribuíram para a divulgação do sistema decimal foi Leonardo de Pisa, também conhecido como Fibonacci, que em 1202 publicou sua obra chamada *Liber Abaci* (O livro do Ábaco), em que explica o uso do sistema decimal. Em 1500 aproximadamente o sistema decimal estava definitivamente aceito na Europa.

O sistema de numeração posicional decimal é também conhecido por *sistema hindu-arábico*, devido à sua origem histórica.

Observamos que o sistema decimal passou por muitas transformações durante sua história. Os símbolos manuscritos dos algarismos tiveram as mais variadas grafias, e se estabilizaram apenas com a invenção da imprensa (cf. Figura 2.7). Também variou a forma de compor e dispor os dígitos de um dado número. Por exemplo, o autor de [113], vol. II, página 77, cita um manuscrito de 1384 em que o número 1384 aparece escrito como 1000.300.80.4, e cita um outro manuscrito em que o número 5782 está escrito na forma 5.7.8.2.

Desde o Século XIII se percebeu ser necessária uma ajuda para facilitar a visualização na grafia de grandes números. Os dígitos do número eram separados em classes, contando da direita para a esquerda. Em geral as classes tinham três dígitos, como ainda se faz hoje, mas foram consideradas classes de seis dígitos, ou ainda quatro dígitos na primeira classe e três em cada uma das classes seguintes.

Seguem alguns exemplos transcritos de [113], vol. II, página 87, que ilustram formas usadas para facilitar a leitura de números grandes.

$$\begin{aligned} \overbrace{678}\ \overbrace{935}\ \overbrace{784}\ \overbrace{105}\ 296 &\qquad \text{(ano de 1202);}\\ \dot{4}.5.9.\dot{3}.6.2.\dot{9}.0.2.2 &\qquad \text{(ano de 1503);}\\ 230|864|089|015|340 &\qquad \text{(ano de 1558).} \end{aligned}$$

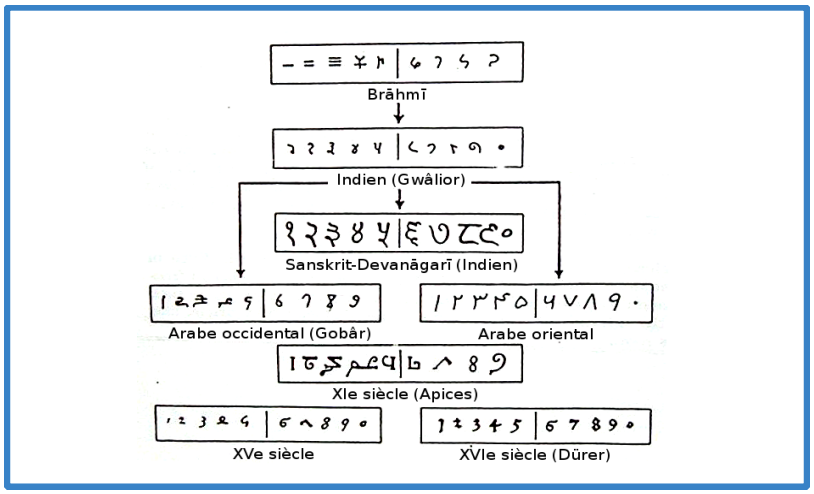



Figura 2.7. O desenho dos símbolos dos algarismos hindu-arábicos passou por muitas modificações ao longo da história. Nessa ilustração, cotada de [27], páginas 105–121, vemos algumas dessas representações.

## 2.10 O sistema de numeração da língua portuguesa

A "Última flor do Lácio, inculta e bela"[1] dá nome aos números naturais seguindo um sistema não posicional, com uma estrutura similar ao sistema alfabético dos antigos gregos e com nomes para os números herdados principalmente da língua latina.

Os *numerais*, na língua portuguesa, constituem um grupo especial de palavras, e podem ser classificados em cardinais, ordinais, multiplicativos e fracionários.

Os **numerais cardinais** são os nomes dos números naturais. Indicam uma quantidade definida de seres ou objetos. Os vocábulos básicos utilizados para nomear os números de zero a 1000 estão indicados na tabela da página 42.

Os numerais de 21 a 99 são compostos justapondo-se a unidade à dezena. Exemplos:

vinte e um (21), cinquenta e nove (59), oitenta e sete (87).

Os numerais de 101 a 999 são compostos justapondo-se a unidade à dezena e esta à centena. Usa-se cento em vez de cem. Não se lê a casa vazia. Intercala-se a conjunção *e* entre as centenas e dezenas e entre estas e a unidade. Exemplos:

cento e trinta e oito (138), duzentos e sete (207), trezentos e noventa e quatro (394).

Para a leitura dos números com mais de três dígitos separamos esses dígitos em grupos de três, a partir da direita, podendo ocorrer que o último grupo fique com um, dois ou três dígitos. Esses grupos de dígitos são denominados *classes*.

As classes são contadas da direita para a esquerda. A primeira classe é chamada *classe das unidades*, a segunda de *classe dos milhares*, a terceira de *classe dos milhões*, e assim por diante, cada classe recebe o nome da menor casa que inicia a classe. A tabela traz, a título de sugestão, nomes para as classes, mas observamos que não existe consenso. Por exemplo, o termo *bilhão*, que no Brasil hoje significa *mil milhões*, representava antigamente *um milhão de milhões*, e conserva esse valor em Portugal e nos países de língua espanhola. Confira observação adicional feita no final da Seção 2.11. Existem também grafias diferentes, por exemplo, alguns dicionários preferem as formas *bilião*, *trilião*, etc.

[1] Olavo Bilac, *Língua Portuguesa*, [15], página 240.

Na leitura de um número as classes são nomeadas da esquerda para a direita (não se usa o conectivo "e" para separar classes). Em cada classe os dígitos são nomeados com as mesmas regras que as dos números de 1 a 999, seguindo-se o nome da classe, exceto a primeira, que não é nomeada.

| | **Numeral cardinal** | | **Numeral cardinal** |
|---|---|---|---|
| 0 | zero | 20 | vinte |
| 1 | um | 30 | trinta |
| 2 | dois | 40 | quarenta |
| 3 | três | 50 | cinquenta |
| 4 | quatro | 60 | sessenta |
| 5 | cinco | 70 | setenta |
| 6 | seis | 80 | oitenta |
| 7 | sete | 90 | noventa |
| 8 | oito | 100 | cem |
| 9 | nove | 200 | duzentos |
| 10 | dez | 300 | trezentos |
| 11 | onze | 400 | quatrocentos |
| 12 | doze | 500 | quinhentos |
| 13 | treze | 600 | seiscentos |
| 14 | quartorze | 700 | setecentos |
| 15 | quinze | 800 | oitocentos |
| 16 | dezesseis | 900 | novecentos |
| 17 | dezessete | 1000 | mil |
| 18 | dezoito | | |
| 19 | dezenove | | |

Segue tabela com nomes sugeridos para as classes:

| | **Nome da classe** | | **Nome da classe** |
|---|---|---|---|
| $10^{3}$ | mil | $10^{33}$ | decilhão |
| $10^{6}$ | milhão | $10^{36}$ | undecilhão |
| $10^{9}$ | bilhão | $10^{39}$ | duodecilhão |
| $10^{12}$ | trilhão | $10^{42}$ | tredecilhão |
| $10^{15}$ | quatrilhão | $10^{45}$ | quatuordecilhão |
| $10^{18}$ | quintilhão | $10^{48}$ | quindecilhão |
| $10^{21}$ | sextilhão | $10^{51}$ | sexdecilhão |
| $10^{24}$ | septilhão | $10^{54}$ | septendecilhão |
| $10^{27}$ | octilhão | $10^{57}$ | octodecilhão |
| $10^{30}$ | nonilhão | $10^{60}$ | novendecilhão |

Exemplos de leitura de números:

1972 um mil novecentos e setenta e dois;

27 309 617 vinte e sete milhões trezentos e nove mil seiscentos e dezessete;

394 938 279 719 trezentos e noventa e quatro bilhões novecentos e trinta e oito milhões duzentos e setenta e nove mil setecentos e dezenove.

Em cada classe, quando necessário, os dígitos podem ser denominados, da direita para a esquerda, como unidades, dezenas e centenas da classe. Por exemplo, em 654 321 temos 4 unidades de milhares, 5 dezenas de milhares e 6 centenas de milhares. Se o dígito é da primeira classe, essa não é nomeada. Assim em 654 321 temos 1 unidade, 2 dezenas e 3 centenas.

Os **numerais ordinais** assinalam o lugar que seres ou coisas ocupam em uma série ordenada. Os vocábulos básicos utilizados para os ordinais estão listados na tabela a seguir.

| | **Numeral ordinal** | | **Numeral ordinal** |
|---|---|---|---|
| | | 20 | vigésimo |
| 1 | primeiro | 30 | trigésimo |
| 2 | segundo | 40 | quadragésimo |
| 3 | terceiro | 50 | quinquagésimo |
| 4 | quarto | 60 | sexagésimo |
| 5 | quinto | 70 | septuagésimo |
| 6 | sexto | 80 | octogésimo |
| 7 | sétimo | 90 | nonagésimo |
| 8 | oitavo | 100 | centésimo |
| 9 | nono | 200 | ducentésimo |
| 10 | décimo | 300 | trecentésimo |
| 11 | undécimo | 400 | quadringentésimo |
| 12 | duodécimo | 500 | quingentésimo |
| 13 | décimo terceiro | 600 | seiscentésimo |
| 14 | décimo quarto | 700 | septingentégimo |
| 15 | décimo quinto | 800 | octingentésimo |
| 16 | décimo sexto | 900 | noningentésimo |
| 17 | décimo sétimo | 1000 | milésimo |
| 18 | décimo oitavo | 1 000 000 | milionésimo |
| 19 | décimo nono | 1 000 000 000 | bilionésimo |

Também se usam décimo primeiro para o ordinal de 11, décimo segundo para o de 12, setuagésimo para o de 70, sexcentésimo para o de 600, setingentésimo para o de 700 e nongentésimo para o de 900.

A representação ordinal dos números é composta aditivamente. Até 2000 a nomenclatura dos ordinais utiliza os nomes da tabela. Na grafia de um número usamos um pequeno círculo superposto e um ponto para indicar que se trata de um ordinal. Exemplos:

29º vigésimo nono;
186º centésimo octogésimo sexto;
1543º milésimo quingentésimo quadragésimo terceiro.

De 2000 em diante a nomenclatura dos ordinais segue outra regra, em que o primeiro numeral é cardinal. Exemplo:

3713º três milésimos septingentésimo décimo terceiro.

Os números redondos constituem exceção: 10 000º décimo milésimo.

Os ordinais variam em gênero e número: primeira da fila; os primeiros a chegar; décima quinta viagem, 29ª. (vigésima nona).

Em alguns casos o ordinal é substituído pelo cardinal correspondente. Na designação de papas, soberanos, séculos, partes de livros e peças, usam-se os ordinais até décimo, e daí por diante o cardinal, sempre que o numeral vier depois do substantivo. Exemplos:

Henrique VIII (lê-se Henrique oitavo); Leão XIII (lê-se Leão treze);
Século X (lê-se Século décimo); Século XI (lê-se Século onze);
Capítulo II (lê-se Capítulo segundo); Capítulo XXVI (lê-se Capítulo vinte e seis).

Quando o numeral antecede o substantivo se usa o ordinal: décimo primeiro século, quadragésimo terceiro capítulo, etc.

Na numeração de artigos de leis, portarias, decretos, usam-se os ordinais até nove, e daí por diante o cardinal. Exemplos:

Artigo 9º (lê-se Artigo nono); Artigo 10 (lê-se Artigo dez).

Na designação dos dias do mês usam-se os cardinais, salvo para o primeiro dia. Na enumeração de casas, apartamentos, cabines, etc. usa-se o ordinal se o numeral vier anteposto, e o cardinal se posposto.

Exemplos:

primeiro de outubro; vinte e sete de maio;

Folha 3 (lê-se folha três); 3ª. folha (lê-se terceira folha).

Os **numerais multiplicativos** designam resultado de multiplicação. Estão listados na tabela abaixo.

Os numerais multiplicativos *dobro, duplo e triplo* são de uso corrente, e os demais costumam ser substituídos pelo cardinal correspondente, seguido da palavra *vezes*. As formas *dúplice* e *tríplice* são adjetivos.

Os numerais multiplicativos, exceto *dobro*, variam em gênero e número. Exemplo: vida dupla.

| **Numeral multiplicativo** | **cardinal correspondente** |
|---|---|
| duplo ou dobro | duas vezes |
| triplo | três vezes |
| quádruplo | quatro vezes |
| quíntuplo | cinco vezes |
| sêxtuplo | seis vezes |
| sétuplo | sete vezes |
| óctuplo | oito vezes |
| nônuplo | nove vezes |
| décuplo | dez vezes |
| undécuplo | onze vezes |
| duodécuplo | doze vezes |
| cêntuplo | cem vezes |

Os **numerais fracionários** designam a parte resultante de divisão por um número natural $\geq 2$.

Os numerais fracionários têm apenas as seguintes formas próprias: meio, ou metade, e um terço. Os demais numerais fracionários são construídos da forma descrita a seguir.

De um quarto a décimo usam-se os ordinais correspondentes, e também para as dezenas e centenas e para mil. Para os outros casos usa-se o cardinal correspondente seguido da palavra *avos*. O numeral fracionário é sempre antecedido de um cardinal que indica a quantidade de partes tomadas. Exemplos:

1/20 um vigésimo;

5/11 cinco onze avos;
1/100 um centésimo.

Na fala a expressão *meia-dúzia*, ou simplesmente *meia*, substitui o cardinal seis quando a clareza se torna importante (ao enunciar números de telefone, por exemplo).

Destacamos finalmente a existência de *substantivos coletivos* que se caracterizam por denotarem um conjunto de seres ou coisas em quantidade determinada. Exemplos: par, biênio, triênio, quadriênio, lustro ou quinquênio, sexênio, setênio, novena, dezena, década ou decênio, duodecênio, dúzia, vintena, centena, cento, centúria, centenário, grosa, milhar, milheiro, milênio, sesquicentenário.

## 2.11 Os números e a legislação brasileira

No Brasil a escrita dos números é regulada pela Resolução nº 12/88 do CONMETRO. Transcrevemos, *ipsis litteris*, o item 3.4.2 dessa Resolução:

*3.4.2 - Os números que representam quantias em dinheiro, ou quantidades de mercadorias, bens ou serviços em documentos para efeitos fiscais, jurídicos e/ou comerciais, devem ser escritos com os algarismos separados em grupos de três, a contar da vírgula para a esquerda e para a direita, com pontos separando esses grupos entre si. Nos demais casos é recomendado que os algarismos da parte inteira e os da parte decimal dos números sejam separados em grupos de três, a contar da vírgula para a esquerda e para a direita, com pequenos espaços entre esses grupos (por exemplo, em trabalhos de caráter técnico ou científico), mas é também admitido que os algarismos da parte inteira e os da parte decimal sejam escritos seguidamente (isto é, sem separação em grupos).*

Neste livro optamos por não usar pontos para separar as classes, mas pequenos espaços para números com seis dígitos ou mais quando for necessário proporcionar mais clareza.

Números de séries especiais podem ter outras grafias. Exemplos:

O telefone da empresa é (976)456-34577654.
O número da agência bancária é 23.001-0.
Resolução nº 12/88 do CONMETRO.

O Brasil é signatário do Sistema Internacional de Pesos e Medidas (SI), no qual existe a chamada regra dos 6N, segundo a qual se passa do milhão ($10^6$) para o bilhão com o acréscimo de seis zeros ($10^{12}$), a trilhão com o acréscimo de mais seis zeros ($10^{18}$), e assim por diante. O Brasil, os Estados Unidos e outros países usam bilhão para $10^9$ desrespeitando com isso o SI.

Para respeitar o SI precisaríamos usar os nomes milhão ($10^6$), mil milhões ($10^9$), bilhão ($10^{12}$), mil bilhões ($10^{15}$), etc.

## 2.12 Problemas adicionais

Na representação de números naturais, se não estiver especificada a base, se trata da base dez.

**Problema 2.12.1.** Os sumérios usavam um sistema posicional de base sessenta, os maias, de base vinte, e os hindus, de base dez. Nossa civilização também escolheu a base dez. Você acha que essa foi a melhor escolha? Por quê? Não seria melhor a base sessenta? ou a vinte?

**Problema 2.12.2.** Descreva pelo menos uma vantagem: **a)** do sistema numérico jônico sobre o hieroglífico egípcio; **b)** do hieroglífico egípcio sobre o romano, **c)** do romano sobre o hieroglífico egípcio; **d)** do sumério sobre o maia; **e)** do decimal sobre o sumério; **f)** do maia sobre o sumério; **g)** do binário sobre o decimal; **h)** do decimal sobre o binário.

**Problema 2.12.3.** Represente 8397 no sistema maia.

**Problema 2.12.4.** Verifique se na língua vernácula a representação dos números cumpre as condições de existência e unicidade. Conforme explicamos na página 5, essas são duas importantes qualidades de um sistema de numeração: a da existência, em que todo número natural tem representação no sistema; e a da unicidade, em que a representação de qualquer número natural no sistema é única. Observamos que um sistema de numeração pode ser muito útil e não possuir essas qualidades.

**Problema 2.12.5.** Explique a seguinte frase. Existem 10 tipos de pessoas: as que conhecem o sistema de numeração binário e as que não conhecem.

**Problema 2.12.6.** Uma escola deseja distribuir R$ 1.234,00 entre seus estudantes mediante prêmios de R$ 1,00, R$ 8,00, R$ 64,00 e R$ 512,00 reais cada. Qual é o menor número de prêmios que se pode atribuir de modo que seja utilizada toda a quantia disponível? Justifique e interprete o resultado.

**Problema 2.12.7.** Um número par tem dez dígitos e a soma desses dígitos é 89. Quais são os valores de todos os dígitos? Explique sua estratégia de solução.

**Problema 2.12.8.** Quantos e quais são os números naturais de 2 algarismos que são iguais ao dobro do produto de seus algarismos?

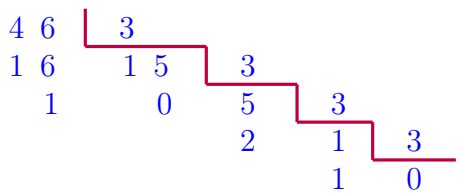
**Problema 2.12.9.** Encontre todos os dígitos decimais $a$ e $b$ tais que $(8ab1)_{dez}$ seja o quadrado de um número natural.

**Problema 2.12.10.** Supondo que 0, 1, 2, 3, 4, ... sejam algarismos de uma certa base $\beta$, descubra todos os valores de $\beta$ que tornam verdadeira a seguinte afirmação: $(14)_\beta \times (14)_\beta = (232)_\beta$.

**Problema 2.12.11.** Descreva as regras necessárias para representar os números no sistema posicional de base quatro em um ábaco (assuma o ábaco descrito no início da Seção 2.4). E em uma base $\beta$ qualquer?

**Problema 2.12.12.** Seja $a$ um número natural cuja representação na base $\beta$ tem $2n$ dígitos. Mostre que $a$ se escreve na forma $a = b + c\beta^n$, sendo $b$ e $c$ números naturais, $c$ com $n$ dígitos e $b$ com uma quantidade de dígitos $\leq n$.

**Problema 2.12.13.** Para transpor 46 para a base três podemos fazer divisões sucessivas da seguinte forma:




(a) Diga qual a representação de 46 na base três e justifique. (b) Use esse método para obter 841 na base quatro.

**Problema 2.12.14. a)** Verifique que para todo $\beta \geq 3$ o número $(121)_\beta$ é quadrado de $(11)_\beta$. **b)** Encontre um número natural $> 1$ na base $\beta$ com todos os dígitos não nulos e que é um cubo de outro número natural para todo $\beta \geq 4$. E quanto a potências quárticas e quínticas? E se dígitos puderem ser zero?

**Problema 2.12.15.** Todo número natural $n$ pode ser escrito como soma de diferentes potências de 2. Por exemplo, $21 = 2^4 + 2^2 + 2^0$ e $37 = 2^5 + 2^2 + 2^0$. **a)** Escreva como soma de potências diferentes de 2 os números: 109; 5937; 71861. **b)** Descreva um ou dois métodos que permitam representar um dado número natural $> 0$ como soma de diferentes potências de 2. **c)** Explique qual é a relação entre a representação binária de um número natural e sua representação como soma de diferentes potências de 2. Sua explicação confirma nossa afirmação inicial, de que todo número natural $n$ pode ser escrito como soma de diferentes potências de 2?

**Problema 2.12.16.** Sejam $a$ um número natural e $\beta \geq 2$ uma base. Usando logaritmos encontre uma fórmula que forneça, em função de $a$ e $\beta$, a quantidade de dígitos da representação de $a$ na base $\beta$.

**Problema 2.12.17.** Ao representar um número natural $a$ na base $\beta$ em um ábaco, colocamos no máximo $\beta - 1$ pedrinhas em cada casa. Se representarmos vários números, tomados aleatoriamente, em média vamos colocar $(\beta - 1)/2$ pedrinhas em cada casa. Sabemos do problema anterior que a quantidade de casas ocupadas para representar $a$ é aproximadamente $\ln(a)/\ln(\beta)$. Portanto, se gastamos 1 segundo para colocar uma pedrinha no ábaco, em média, então, em média gastamos

$$\frac{\ln(a)}{2}\,\frac{\beta - 1}{\ln(\beta)}$$

segundos para representar $a$. Fixado $a$, encontre a base $\beta$ que proporciona menor gasto de tempo.

**Problema 2.12.18. a)** Verifique que se um número tem $d$ dígitos no sistema decimal, então no sistema binário terá aproximadamente $3{,}32\,d$ dígitos. **b)** Verifique que se um número tem $d$ dígitos no sistema decimal, então no sistema sexagesimal terá um pouco mais da metade, aproximadamente $0{,}56\,d$.

**Problema 2.12.19.** Determine a quantidade total de dígitos (decimais) que são escritos ao se representar um a um os números naturais 1, 2, 3, ..., $10^n$.

**Problema 2.12.20.** Um linotipista dispõe de 500 tipos de cada um dos dez algarismos decimais e pretende imprimir de uma vez os números naturais, um a um, a partir de 1, até $N$. Qual é o maior valor possível de $N$?

**Problema 2.12.21.** Em um processo de codificação, qualquer número natural $n$ com até nove dígitos é relacionado ao número/código $(abc)_{dez}$, em que $a$ é o número de dígitos de $n$, $b$ é o número de dígitos ímpares de $n$ e $c$ é o número de dígitos pares de $n$. (i) Encontre um número cujo número/código é ele mesmo. (ii) Se codificarmos um número/código, o que iremos encontrar?

**Problema 2.12.22.** Afinal, dígito e algarismo são sinônimos? Justifique sua resposta.

## 2.13 Sugestões de atividades

**Atividade 2.13.1.** Examinando os sistemas de numeração aditivos estudados no Capítulo 1, identifique em que situações eles usam ou não os recursos de posição e agrupamento.

**Atividade 2.13.2.** Faça uma pesquisa sobre o valor do termo *bilhão* nos mais diversos países.

**Atividade 2.13.3.** Pesquise quais são os sistemas numéricos usados correntemente nos mais diversos países na atualidade. Particularmente descubra se existem países que adotam o sistema decimal mas nos quais a grafia dos algarismos seja diferente da nossa.

**Atividade 2.13.4.** Pesquise em livros de História da Matemática o antigo sistema de numeração chinês em barras assim como o sistema de agrupamentos multiplicativos chinês-japonês.

**Atividade 2.13.5.** Obtenha na Internet uma Tabela ASCII e estude os valores decimais, binários e hexadecimais ali usados.

**Atividade 2.13.6.** Em nossa civilização os números são frequentemente usados como código. Por exemplo, nos sistemas de telefonia os números são tomados como símbolos, e não importa seu valor. Em outras situações o valor é usado parcialmente, por exemplo quando existem dígitos verificadores. Faça uma pesquisa sobre esse assunto.

**Atividade 2.13.7.** As cédulas e moedas do sistema monetário brasileiro precisam obedecer a um sistema decimal para haver coerência com a legislação que regula a escrita dos valores. Mas, para facilitar o uso cotidiano, existem cédulas e moedas de valores intermediários. Descreva algebricamente esse sistema.

**Atividade 2.13.8.** Faça na internet ou em outras fontes uma pesquisa sobre a história do ábaco. Estude os diversos tipos de ábacos utilizados pela humanidade. Inclua em seu resumo considerações de especialistas em ensino da Matemática sobre a importância (ou não) de incluir o uso do ábaco na escola básica para melhor compreensão dos sistemas de numeração. Não deixe de fazer suas próprias considerações.



Figura 2.8. À esquerda, foto de um ábaco escolar. À direita, foto de um ábaco russo.

**Atividade 2.13.9.** Ainda sobre ábacos, você acha que o ábaco com separação, como o que está ilustrado na Figura 2.9, pode ser considerado um ábaco decimal? Você pode desenvolver uma representação algébrica para esse ábaco?

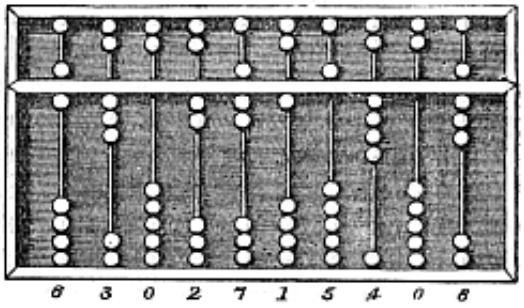



Figura 2.9. Desenho de um tipo comum de ábaco com separação. Uma conta na região superior de uma casa vale 5 vezes uma conta da região inferior. As contas acionadas são as que se encontram junto à haste de separação. Está sendo representado o número

$$6\,302\,715\,408.$$

**Atividade 2.13.10.** Pesquise em um dicionário os significados indicados pelas palavras: par, biênio, triênio, quadriênio, lustro ou quinquênio, sexênio, setênio, novena, dezena, década ou decênio, duodecênio, dúzia, vintena, centena, cento, centúria, centenário, grosa, milhar, milheiro, milênio, sesquicentenário.

**Atividade 2.13.11.** Em um livro de Matemática para professores pode-se ler a frase (adaptada): "As principais motivações para o desenvolvimento da Matemática são as necessidades práticas e operacionais". Faça uma análise desse discurso.

**Atividade 2.13.12.** Em um livro de Matemática para professores pode-se ler o seguinte (adaptado): "O sistema de numeração que utilizamos demorou séculos para ser desenvolvido. Isso nos dá uma ideia de que esse sistema de numeração não é simples, e que sua compreensão pelas crianças deve ser cuidadosamente desenvolvida".

Faça uma análise do que ocorre no ensino do sistema decimal nas escolas fundamentais, pesquisando na literatura especializada ou fazendo suas próprias investigações.

# Capítulo 3

# A arte de calcular

## 3.1 Introdução

O que são as operações da Aritmética?

O que são algoritmos para essas operações?

Como calcular em bases não decimais?

Apresentamos, neste capítulo, as quatro operações fundamentais da Aritmética, a saber, a *adição*, a *subtração*, a *multiplicação* e a *divisão*. Dedicar-nos-emos particularmente ao estudo dos conceitos dessas operações e da gênese dos algoritmos usualmente utilizados para implementá-las. Veremos também alguns detalhes da *potenciação*.

Designar essas quatro operações como *operações fundamentais* é um costume de nossa época. Na História da Matemática a ideia de operação fundamental passou por várias mudanças. De acordo com [113], volume II, página 32, na primeira metade do segundo milênio eram consideradas, na Europa, sete operações fundamentais, às vezes nove, a saber: numeração, adição, subtração, duplicação, mediação, multiplicação, divisão, progressão e radiciação. Nesse contexto numeração significa contar, ou enumerar, progressão significa potenciação, e mediação, divisão por dois. A duplicação e a mediação eram incluídas como operações fundamentais em virtude de serem a base de antigos algoritmos para a multiplicação e a divisão.

Conforme veremos, a enumeração dá origem à adição, e essa, por sua vez, gera todas as outras operações.

Ao estudarmos os algoritmos das operações temos em mente que o leitor já conhece os denominados algoritmos usuais, aqueles que são ensinados na escola básica e que são correntemente aplicados quando necessitamos implementar um cálculo através da escrita em papel. Portanto nosso escopo não é ensinar esses algoritmos mas proporcionar uma reflexão sobre sua origem e sequências didáticas para seu ensino. A descrição algébrica e geral desses algoritmos não é feita neste texto e é apenas sugerida em alguns problemas.

## 3.2 A adição

A adição é a primeira operação fundamental da Aritmética, e dela derivam todas as outras.

### 3.2.1 Conceito de adição

Vimos na página 4 que todo número natural $a$ tem um único sucessor, indicado por $a+1$. Definimos a adição de um número natural $a$ com a unidade como a operação da qual resulta o sucessor de $a$.

Podemos estender esse conceito, e definir a adição de um número natural $a$ com um número natural qualquer $b$: ao número $a$ adicionamos tantas unidades quantas são as unidades do número $b$. Mais exatamente, a adição de $a$ e $b$ é a operação da qual resulta um número natural definido da seguinte forma: tomamos o sucessor $a+1$ de $a$, em seguida o sucessor de $a+1$, e assim por diante, realizamos a ação "tomar o sucessor" tantas vezes quantas são as unidades de $b$.

Por exemplo, para adicionar dois a três, fazemos, sucessivamente,

$$(1+1+1)+1 = 1+1+1+1 \quad \text{e} \quad (1+1+1+1)+1 = 1+1+1+1+1,$$

e o resultado é cinco.

Fica assim determinada a *operação de adição*, que associa a dois números naturais $a$ e $b$ um terceiro número natural $c$, chamado *soma* de $a$ e $b$. Indicamos a soma de $a$ e $b$ por $a+b$ ( lê-se: a mais b ). *Adicionar* ou *somar* $a$ e $b$ significa calcular $a+b$.

A operação de adição pode também ser entendida como uma reunião. Dados números naturais $a$ e $b$, consideramos uma cesta com $a$ bolinhas e uma segunda cesta com outras $b$ bolinhas. Reunindo as bolinhas em uma única cesta, a quantidade de bolinhas nessa última é $a+b$.

Observemos que a operação de adição satisfaz duas importantes propriedades: comutatividade e associatividade.

A *propriedade comutativa da adição* significa que dados quaisquer números naturais $a$ e $b$ se tem $a+b=b+a$. Dessa forma para encontrar a soma $a+b$ podemos proceder de duas maneiras: começar com $a$ e tomar os sucessores $a+1$, $a+1+1$, ... ($b$ vezes), ou começar com $b$ e tomar os sucessores $b+1$, $b+1+1$, ... ($a$ vezes). Para se convencer da validade dessa propriedade o estudante pode fazer a seguinte imagem. Considere dois cestos $A$ e $B$ com $a$ e $b$ bolinhas respectivamente. Tome uma a uma as bolinhas de $B$ e as coloque em $A$. Quando terminar, a quantidade de bolinhas em $A$ é $a+b$. Depois faça o contrário: tome uma a uma as bolinhas de $A$ e as coloque em $B$. Quando terminar, a quantidade de bolinhas em $B$ é $b+a$. Como as quantidades resultantes são as mesmas, então $a+b=b+a$.

A *propriedade associativa da adição* significa que dados quaisquer números naturais $a$, $b$ e $c$ se tem $(a+b)+c=a+(b+c)$. Isso significa que para adicionar três números $a$, $b$ e $c$ podemos proceder de duas maneiras: primeiro adicionar $a$ com $b$, tomar o resultado e adicionar a $c$; ou então primeiro adicionar $b$ com $c$, tomar o resultado e adicionar a $a$. A propriedade associativa afirma que o número resultante é o mesmo. O estudante pode se convencer da validade dessa afirmação tomando três cestas $A$, $B$ e $C$ com $a$, $b$ e $c$ bolinhas respectivamente, e imaginando os dois procedimentos.

Destacamos essas duas propriedades da seguinte forma:

*Quaisquer que sejam os números naturais $a$, $b$ e $c$, temos*

$$a+b=b+c \qquad \text{e} \qquad (a+b)+c=a+(b+c). \tag{3.1}$$

Observamos que podemos definir a adição de três ou mais números naturais. Por exemplo, para três números a definição ficaria assim: quaisquer que sejam os números naturais $a$, $b$ e $c$,

sua *soma* é $a+b+c=(a+b)+c$. As propriedades comutativa e associativa implicam que não importa a ordem com que os números são somados.

Na adição os números que estão sendo adicionados chamam-se *termos* ou *parcelas*, e o número que resulta da operação chama-se *soma* ou *total*.

### 3.2.2 Algoritmos para a adição

*Efetuar* a operação de adição em um sistema de numeração significa obter e representar, nesse sistema, a soma de dois ou mais números naturais. O mesmo significado tem as expressões *calcular a soma*, *somar* ou *adicionar*.

Chamamos de *algoritmo para a adição* a qualquer método que permite calcular a soma de dois ou mais números em um sistema de numeração.

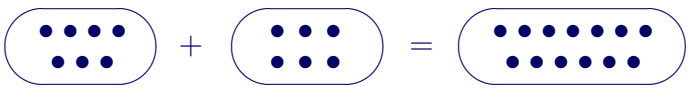
Os algoritmos mais simples que podem ser utilizados para efetuar a operação de adição constituem aplicação imediata dos dois conceitos de adição: "acrescentar" e "reunir".

Por exemplo, dados os números $a=7$ e $b=6$ no sistema decimal, vamos calcular a sua soma acrescentando as unidades de $b$ às unidades de $a$, uma a uma. Temos:

$$\begin{array}{rcll} 7+1 & = & 8 & \text{(uma vez)},\\ 8+1 & = & 9 & \text{(duas vezes)},\\ 9+1 & = & 10 & \text{(três vezes)},\\ 10+1 & = & 11 & \text{(quatro vezes)},\\ 11+1 & = & 12 & \text{(cinco vezes)},\\ 12+1 & = & 13 & \text{(seis vezes)}. \end{array}$$

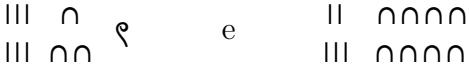
Portanto, $7+6=13$ no sistema decimal. Vemos que, para somar, teoricamente precisamos apenas saber contar, ou saber "tomar o sucessor".

Por outro lado, para efetuar $7+6$ tendo em vista que a adição é uma reunião, tomamos uma cesta $A$ com 7 bolinhas e uma cesta $B$ com 6 bolinhas (ou desenhamos essas bolinhas), reunimos e contamos. O resultado é novamente 13.



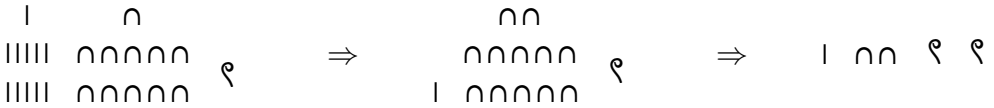
Quando precisamos somar números maiores percebemos a necessidade de desenvolver algoritmos rápidos e compactos para a adição. Imagine o que seria efetuar $1735+1463$ "tomando o sucessor", ou usando bolinhas!

Interessa-nos estudar os algoritmos de adição para o sistema decimal. Mas como muitos estudantes têm curiosidade em saber como efetuar a adição nos sistemas egípcio e romano, vejamos um exemplo em cada um desses sistemas de numeração. Nos sistemas aditivos o método da reunião parece ser mais conveniente. Para calcular $136+85$ no sistema hieroglífico egípcio, começamos representando esses números:

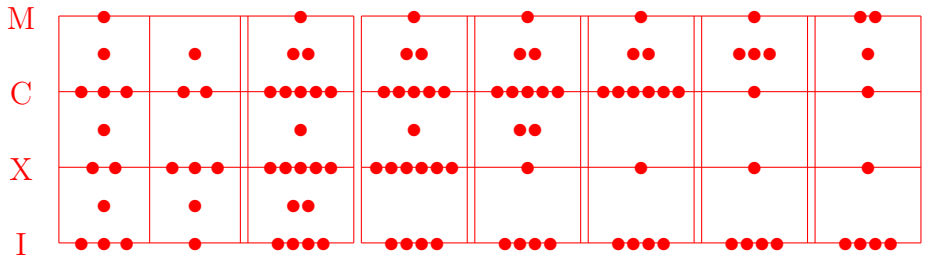


Em seguida agrupamos os símbolos do mesmo tipo, e substituímos cada dez deles por um

de valor dez vezes maior. O resultado é 221, como se vê a seguir:



A adição no sistema romano era usualmente implementada em ábacos seguindo essa mesma técnica de ajuntamento. Vemos abaixo uma forma de obter a soma de MDCCCLXXVIII com DCCXXXVI em um ábaco romano com duas colunas e sulcos horizontais. Desenhamos colunas adicionais para representar os movimentos realizados com as pedrinhas na segunda coluna.




Na primera coluna está representado o número MDCCCLXXVIII, e na segunda, DCCXXXVI. Observe que uma pedrinha colocada entre dois sulcos representa cinco pedrinhas colocadas no sulco imediatamente abaixo, e duas pedrinhas colocadas entre dois sulcos equivalem a uma pedrinha colocada no sulco imediatamente acima. No primeiro desenho adicional da segunda coluna vemos o primeiro movimento do cálculo, que consiste no ajuntamento das pedrinhas das colunas um e dois de uma mesma linha. Representamos nas outras colunas do desenho os movimentos seguintes, em que rearranjamos os grupos de pedrinhas de baixo para cima. O resultado é MMDCXIIII, ou MMDCXIV. Certamente que outras opções de rearranjo são possíveis.

Os romanos também escreviam usando uma tábua coberta com cera e um estilo. A adição $59 + 552 = 611$ exemplificada a seguir poderia muito bem ter sido feita por um antigo romano.

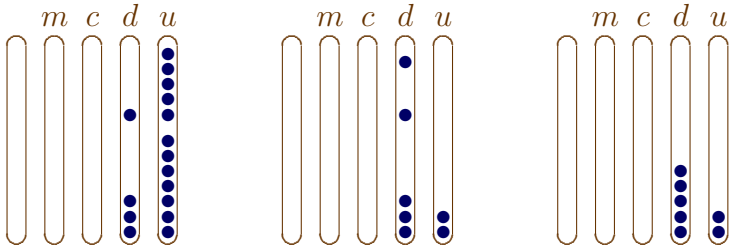
| | |
|---|---|
| LIX | |
| DLII | |
| DLLVIIIIII | (soma provisória: ajuntamento dos símbolos) |
| DLLVVI | (rearranjo) |
| DCXI | (soma final) |

### 3.2.3 Gênese dos algoritmos de adição para sistemas posicionais

O uso corrente da adição nas mais diversas aplicações exigiu o desenvolvimento de algoritmos compactos e rápidos para somar números naturais. Inicialmente o ábaco era o instrumento mais disponível para implementar as operações aritméticas. Particularmente a adição pode ser efetuada em um ábaco mediante o ajuntamento das pedrinhas e seu reajuste de modo que em cada casa não fique mais do que nove pedrinhas.

Vejamos como efetuar $15 + 37$ em um ábaco. Primeiro representamos 15 e 37, como na figura abaixo, à esquerda. As pedrinhas estão separadas, de modo que na parte de baixo está representado 37, e na parte de cima, 15 (poderia ser o contrário). Lembrando que dez pedrinhas na primeira casa equivalem a uma pedrinha na segunda casa, fazemos o acerto: tiramos dez pedrinhas da primeira casa e colocamos uma na segunda. O resultado é $15+37 = 52$,

representado na figura da direita, abaixo.




Para nossos estudos interessa implementar a adição na linguagem escrita. O estudante já conhece nossa forma usual de implementar $15 + 37$:

$$\begin{array}{r} 15 \\ +37 \\ \hline 52 \end{array}$$

que representa as seguintes etapas de cálculo:

$$\begin{array}{r} 15 \\ +37 \\ \hline \end{array} \longrightarrow \begin{array}{r} {\scriptstyle 1 \leftarrow \text{transporte}} \\ 15 \\ +37 \\ \hline 2 \end{array} \longrightarrow \begin{array}{r} 15 \\ +37 \\ \hline 52 \end{array}$$

O estudante pode examinar a sequência de cálculos dispostos acima e verificar que ela imita os movimentos realizados no ábaco.

Na linguagem escolar a unidade transportada para a casa seguinte denomina-se "um de reserva". Também se diz "vai um".

Nosso dispositivo usual de adição não é a única forma de transpor para a linguagem escrita o que é feito no ábaco. Um antigo dispositivo hindu pode ser visto no exemplo abaixo, em que calculamos $731 + 492$. O estudante pode imaginar os movimentos correspondentes do ábaco.

$$\begin{array}{r} 731 \\ 492 \\ \hline \end{array} \rightarrow \begin{array}{r} 733 \\ 49 \\ \hline \end{array} \rightarrow \begin{array}{r} 823 \\ 4 \\ \hline \end{array} \rightarrow \begin{array}{r} 1223 \\ \\ \hline \end{array}$$

Outras variações do método usual, provenientes ou não do ábaco, podem ter interesse histórico e pedagógico. Vamos apresentar algumas delas, começando com a chamada "versão longa", muito usada na Europa no Século XVI.

$$\begin{array}{r} 731 \\ +492 \\ \hline 3 \\ 12 \\ 11 \\ \hline 1223 \end{array}$$

Este é também um antigo método hindu. A soma começa a ser feita pela esquerda, e os dígitos vão sendo corrigidos à medida que for necessário.

$$\begin{array}{r} 731 \\ +492 \\ \hline 1123 \\ 2 \end{array}$$

Os métodos de adição dos árabes seguiam de perto os métodos hindus. Vejamos três exemplos. No primeiro a soma é feita da direita para a esquerda. Os dígitos 1 da operação "vai um"

são guardados na última linha.

$$\begin{array}{r} 72373 \\ 3318 \\ 514 \\ \hline 76205 \\ \hline 111 \end{array}$$

Neste segundo exemplo a soma é feita da esquerda para a direita. O primeiro resultado é provisório, logo abaixo dele são guardados os dígitos de reserva. Em seguida são somados esses dígitos. Essa última soma foi feita da direita para a esquerda.

$$\begin{array}{r} 53732 \\ 4179 \\ 6105 \\ \hline 53906 \\ 1\ \ 11\ \ \\ \hline 64016 \end{array}$$

Neste último exemplo de antigo método árabe de adição o resultado é colocado na linha superior. À direita estão os dígitos obtidos com a aplicação da prova do nove (confira página 85).

$$\begin{array}{|r|r|} \hline 8030 & 2 \\ \hline 5687 & 8 \\ 2343 & 3 \\ \hline \end{array}$$

Lembramos o leitor de que o ábaco e a linguagem escrita não são os únicos métodos de somar. Podemos somar sem nada registrar, guardando os dados intermediários na memória. Por exemplo, para implementar $731 + 492$, fazemos $700 + 500 = 1200$, a esse valor adicionamos 30, obtendo 1230, em seguida retiramos 8, o que dá 1222, e finalmente somamos 1, do que resulta 1223. Esse tipo de procedimento é denominado *técnica mental* de adição.

Pode ocorrer ainda de estarmos interessados no valor aproximado de uma soma. Por exemplo, se um livro custa 37 reais e outro 29, queremos saber se os 70 reais que temos no bolso são suficientes para pagar. Não é necessário calcular $37 + 29$, basta ver que $40 + 30 = 70$. Muitos especialistas em ensino da Matemática têm afirmado que no ensino formal da aritmética é importante desenvolver técnicas de *cálculo aproximado*.

Os mesmos algoritmos e dispositivos utilizados para efetuar a adição no sistema decimal podem ser implementados em qualquer sistema posicional. Vamos exemplificar com o sistema posicional de base sete. A adição abaixo foi feita nesse sistema.

$$\begin{array}{r} {\scriptstyle 1\ \ 1\ \ } \\ 1\ 3\ 5 \\ +\ 2\ 6\ 4 \\ \hline \\ 4\ 3\ 2 \end{array}_{sete}$$

O mecanismo do algoritmo é exatamente o mesmo do algoritmo usual de adição do sistema decimal. Ocorre apenas que a soma de dois algarismos quaisquer deve ser feita na base sete. Para calcular $5 + 4$ podemos proceder por contagem: $5 + 1 = 6$, $6 + 1 = 10$, $10 + 1 = 11$ e $11 + 1 = 12$. Portanto $5 + 4 = 12$ na base sete. Podemos também utilizar temporariamente a base dez: $5 + 4 = 9$, e $9 = 1 \cdot 7 + 2 = (12)_{sete}$. Portanto $5 + 4 = 12$ na base sete.

Quando fazemos uma adição no sistema decimal utilizamos automaticamente as informações que temos na memória desde a infância, que são as somas de todos os algarismos. É o que chamamos de memorizar a *tábua de adição*. Dessa forma para fazer um cálculo de adição na base sete mais confortavelmente é bom termos em mãos a tábua de adição na base sete, como segue.

| $+_{sete}$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| 1 | 1 | 2 | 3 | 4 | 5 | 6 | 10 |
| 2 | 2 | 3 | 4 | 5 | 6 | 10 | 11 |
| 3 | 3 | 4 | 5 | 6 | 10 | 11 | 12 |
| 4 | 4 | 5 | 6 | 10 | 11 | 12 | 13 |
| 5 | 5 | 6 | 10 | 11 | 12 | 13 | 14 |
| 6 | 6 | 10 | 11 | 12 | 13 | 14 | 15 |

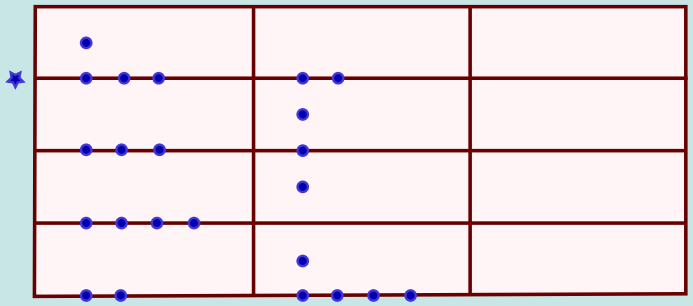
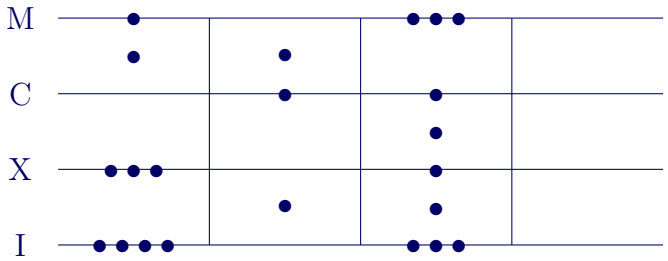


Figura 3.1 Representação estilizada de um ábaco como era utilizado na Europa no século XVI, conforme está descrito no livro *Ground of Arts*, de Robert Recorde, publicado na Inglaterra em 1542. Cada linha horizontal representa uma casa do sistema decimal. A linha inferior representa a casa das unidades, e a linha assinalada com $\star$ é a casa dos milhares. Uma conta colocada entre duas linhas equivale a cinco contas posicionadas na linha imediatamente abaixo. Na figura o número 8342 está representado na primeira coluna da esquerda, e 2659 na coluna do meio. O ábaco está pronto para que seja executado o cálculo de $8342 + 2659$ ou $8342 - 2659$. Informações extraídas de [113], volume II, página 184 e seguintes.

### 3.2.4 Problemas

**Problema 3.2.4.1.** Implemente a adição dos três números abaixo como se fosse no ábaco romano. Use também linguagem escrita.




**Problema 3.2.4.2.** Encontre várias formas de efetuar $27 + 18$.

**Problema 3.2.4.3.** Na adição de três parcelas pode ocorrer um "vai dois", como no exemplo

$$\begin{array}{r} {\scriptstyle 2\ \ \ } \\ 5\,3\,7 \\ +\,6\,2\,9 \\ \hline 1\,3\,8\,1 \end{array}$$

**a)** Verifique que na adição de duas parcelas nunca ocorre um "vai dois", ou mais. **b)** Investigue o que ocorre na adição de três parcelas, quatro parcelas, etc. **c)** Um estudante estava adicionando algumas parcelas simultaneamente, e aconteceu um "vai doze". Em que casa deve ser somado esse doze?

**Problema 3.2.4.4.** Verifique em quais aspectos a versão longa da adição é mais simples do que o método usual, e em quais não é. Verifique se a versão longa evita o uso do "vai um". Será que esse método deveria ser apresentado para os estudantes nas escolas antes do método usual?

**Problema 3.2.4.5.** Comparando o nosso algoritmo usual de adição com suas variações descritas nesta seção, verifique qual é a que está melhor adaptada à linguagem escrita e qual proporciona maior economia de tempo.

**Problema 3.2.4.6.** Calcule $343 + 489$ mentalmente de várias formas de modo a obter: **a)** respostas aproximadas; **b)** a resposta exata.

**Problema 3.2.4.7.** Ao calcular $343 + 489$ mentalmente temos a tendência de iniciar com as centenas: $300 + 400 = 700$. Por que então o algoritmo usual inicia a soma pela coluna das unidades?

**Problema 3.2.4.8.** Em um antigo manuscrito hindu lê-se o seguinte:

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| soma das unidades: | 2 | 5 | 2 | 3 | 8 | 0 | 0 | | 2 0 |
| soma das dezenas: | | | 3 | 9 | 1 | 1 | 0 | | 1 4 |
| soma das centenas: | | | | 1 | 0 | 0 | 1 | | 2 |
| soma das somas: | | | | | | | | | 3 6 0 |

Quais números foram somados? Como foi feita a soma?

**Problema 3.2.4.9.** Um arqueólogo viu num estranho manuscrito um conjunto de símbolos que interpretou como

$$\text{ßßßßI} + \text{ßßß} = \text{ßßßßßßßßI}$$

O que poderia ser isso?

**Problema 3.2.4.10.** Em um manuscrito do tempo de Bhaskara foi encontrado o seguinte cálculo. Decifre.

$$\begin{array}{r} 542071 \\ 469892 \\ 5277 \\ 73085 \\ \hline 1090325 \\ \hline 12131 \end{array}$$

**Problema 3.2.4.11.** Faça o cálculo abaixo da esquerda para a direita. Qual é o resultado? Esse método é mais fácil que o usual, em que se procede da direita para a esquerda?

$$\begin{array}{r} 6\,5\,8\,9\,1 \\ +\,2\,3\,4\,7\,9 \\ \hline 1\,1\,6\,9\,0 \end{array}$$

**Problema 3.2.4.12.** Aproveite a tábua de adição na base sete na página 57, e efetue de várias maneiras diferentes:

$$(254)_{sete} + (103)_{sete}\,;$$
$$(2344)_{sete} + (5642)_{sete}\,;$$
$$(40563)_{sete} + (6301)_{sete} + (56314)_{sete}\,.$$

Faça os cálculos também em um ábaco.

**Problema 3.2.4.13.** Observe as propriedades de simetria e regularidade em uma tábua de adição. Utilizando essas propriedades construa as tábuas de adição nas bases cinco, oito e doze. Efetue nas bases indicadas:

$$(4021)_{cinco} + (2321)_{cinco}\,;$$
$$(76032)_{oito} + (54021)_{oito}\,;$$
$$(9A305)_{doze} + (6AB56)_{doze}\,.$$

**Problema 3.2.4.14.** Construa a tábua de adição da base dois. Confira o seguinte cálculo nessa base:

$$\begin{array}{r} 1\,1\,0\;\;0\,0\,0\;\;1\,0\,0\;\;1\,1\,1\;\;1\,0\,1\;\;1\,1\,0 \\ +\quad 1\;\;0\,1\,1\;\;1\,0\,0\;\;0\,0\,0\;\;0\,0\,0\;\;1\,0\,1 \\ \hline 1\,1\,1\;\;1\,0\,0\;\;0\,0\,0\;\;1\,1\,1\;\;1\,1\,0\;\;0\,1\,1 \end{array}$$

## 3.3 A subtração

A subtração é inversa da adição. Enquanto a adição está relacionada com os conceitos de *acrescentar* e *juntar*, a subtração corresponde a *retirar* e *completar*.

### 3.3.1 Conceito de subtração

Conforme já vimos, o *antecessor* de um número natural $a \neq 1$ é o número natural cujo sucessor é $a$. Por exemplo, o antecessor de 2 é 1, de 3 é 2, de 4 é 3, e assim por diante.

Indicamos o antecessor de $a$ por $a-1$ (lê-se: a menos um). Portanto, obtemos o antecessor de um número retirando uma de suas unidades. A ação "tomar o antecessor de um número natural" é inversa da ação "tomar o sucessor de um número natural".

Se $a$ e $b$ são dois números naturais tais que $a$ tem mais unidades do que $b$, podemos *subtrair* $b$ *de* $a$ retirando de $a$ tantas unidades quantas as que são de $b$. Por exemplo, para subtrair cinco de doze, consideramos as unidades de doze

$$1+1+1+1+1+1+1+1+1+1+1+1,$$

das quais retiramos cinco, e ficamos com

$$1+1+1+1+1+1+1,$$

que é sete. Portanto, subtraindo-se cinco de doze, resulta sete. Representamos esse fato com a notação

$$12-5=7.$$

Mais geralmente, se $b$ tem menos unidades do que $a$, o resultado de subtrair $b$ de $a$ é indicado por $a-b$ (lê-se: a menos b), e é chamado *diferença* entre $a$ e $b$.

Fica assim determinada a *operação de subtração*. Deixamos claro também que a subtração é inversa da adição. Isso significa que se subtrairmos $b$ de $a$ e depois, ao resultado, adicionarmos $b$, obtemos novamente $a$. Em outros termos,

$$(a-b)+b=a. \tag{3.2}$$

Do mesmo modo, se adicionarmos $a$ e $b$, e da soma subtrairmos $b$, o resultado é $a$:

$$(a+b)-b=a. \tag{3.3}$$

Observamos que, para subtrair, necessitamos de apenas uma habilidade matemática: saber contar.

A subtração pode ser estudada também através de sua relação com o conceito de completar. Se temos uma cesta com 12 bolinhas e outra com cinco bolinhas, queremos saber quantas bolinhas devemos acrescentar na segunda cesta para que a quantidade de bolinhas fique igual à da primeira.

Com essa ideia as crianças fazem subtrações usando os dedos das mãos. Para calcular $12-5$ contam "seis", e abaixam um dedo, "sete", e abaixam outro dedo, a assim por diante, até chegar a doze. Os dedos abaixados perfazem sete, e desse modo $12=5+7$, o que equivale a $12-5=7$. Dessa forma, dados números naturais $a$ e $b$ tais que $a$ tem mais unidades do que $b$, a diferença $a-b$ é o número natural que somado com $b$ resulta $a$, ou seja, temos novamente $a=b+(a-b)$.

Vejamos algumas fórmulas e propriedades algébricas que serão úteis.

*Lei de Cancelamento da adição:* quaisquer que sejam os números naturais $a$, $b$ e $c$, temos

$$a+c=b+c \iff a=b. \tag{3.4}$$

De fato, se $a+c=b+c$, temos $(a+c)-c=(b+c)-c$ (pois estamos subtraindo $c$ do mesmo número). Usando (3.3) vem $a=b$. Reciprocamente, se $a=b$ temos $a+c=b+c$, pois estamos adicionando $c$ ao mesmo número.

*Lei de Cancelamento da subtração:* quaisquer que sejam os números naturais $a$, $b$ e $c$, se $c$ tem menos unidades do que $a$ e do que $b$, temos

$$a-c=b-c \iff a=b. \tag{3.5}$$

De fato, se $a-c=b-c$, temos $(a-c)+c=(b-c)+c$ (pois estamos adicionando $c$ ao mesmo número). Usando (3.2) vem $a=b$. Reciprocamente, se $a=b$ temos $a-c=b-c$, pois estamos subtraindo $c$ do mesmo número.

Quaisquer que sejam os números naturais $a$, $b$ e $c$, se $b$ e $c$ têm menos unidades do que $a$, temos

$$a-b=c \iff a=b+c \iff a-c=b. \tag{3.6}$$

De fato, se $a - b = c$, temos $(a - b) + b = b + c$ (pois estamos adicionando $b$ ao mesmo número). Usando (3.2) vem $a = b + c$. Reciprocamente, se $a = b + c$ temos $a - b = (b + c) - b$, pois estamos subtraindo $b$ do mesmo número. Usando (3.3) vem $a - b = c$. Agora, trocando $b$ e $c$ de lugar, $a - c = b \iff a = b + c$ é a mesma afirmação, e obtemos todas as implicações.

Com essas observações podemos justificar as regras algébricas usadas pelos estudantes ao lidar com equações que envolvem adição e subtração de números naturais. Vejamos mais dois exemplos.

Quaisquer que sejam os números naturais $a$, $b$ e $c$, se $c$ tem menos unidades do que $b$, temos

$$a + (b - c) = (a + b) - c. \tag{3.7}$$

De fato, seja $d = b - c$. Por (3.6) temos $b = c + d$. Logo $a + b = a + (c + d)$. Rearranjando temos $a + b = (a + d) + c$. Subtraindo $c$ de ambos vem $(a + b) - c = [(a + d) + c] - c = a + d$, e aqui usamos (3.3). Portanto $(a + b) - c = a + d = a + (b - c)$, e terminamos a justificativa.

Sejam $a$, $b$ e $c$ números naturais tais que $b$ tem menos unidades do que $a$ e $c$ tem menos unidades do que $b$. Então

$$(a - c) - (b - c) = a - b. \tag{3.8}$$

Para justificar essa fórmula, notemos primeiro que $c$ tem menos unidades do que $a$ e $b - c$ tem menos unidades do que $a - c$, portanto podemos fazer o cálculo $(a - c) - (b - c)$. Seja $m = (a - c) - (b - c)$. Usando (3.6) vem $m + (b - c) = a - c$. De (3.7) vem $(m + b) - c = a - c$. Cancelando $c$ temos $m + b = a$, e $m = a - b$ (por (3.6)). Lembrando o que é $m$, obtemos $(a - c) - (b - c) = a - b$, como queríamos.

Por último, sejam $a$, $b$ e $c$ os números naturais tais que $b$ tem menos unidades do que $a$. Então

$$(a + c) - (b + c) = a - b. \tag{3.9}$$

Para justificar essa fórmula, notemos primeiro que $b + c$ tem menos unidades do que $a + c$, portanto podemos fazer o cálculo $(a + c) - (b + c)$. Seja $n = (a + c) - (b + c)$. Usando (3.6) vem $n + (b + c) = a + c$. Usando a associativa da adição vem $(n + b) + c = a + c$. Cancelando $c$ temos $n + b = a$, e $n = a - b$ (por (3.6)). Lembrando o que é $n$, obtemos $(a + c) - (b + c) = a - b$, como queríamos.

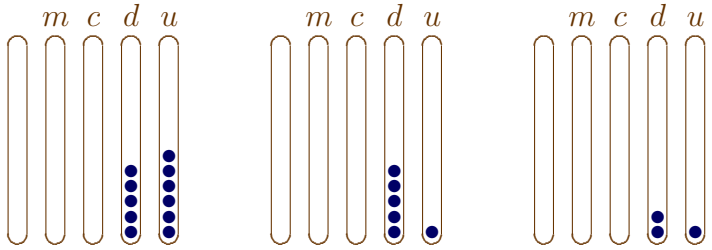
*Observamos* que essas "regras de equações algébricas" são de conhecimento prévio do estudante. Na lista de Problemas 3.3.3, apresentamos mais algumas. Apenas chamamos a atenção para o seguinte fato: nesse ponto de nossos estudos, o sinal "-" só pode ser usado para indicar subtração. Posteriormente, com a definição de números inteiros negativos, uma expressão como $-(b - c)$ pode ser interpretada como $(-1) \cdot (b - c)$, e a regra de troca de sinais nos permitirá escrever $-(b - c) = -b + c$.

### 3.3.2 Algoritmos para a subtração

Vimos que para calcular a diferença entre números naturais basta saber contar, e demos um exemplo calculando $12 - 5$. Mas esse método é inviável para números grandes, por exemplo, para calcular $358 - 297$. Devido a isso necessitamos de algoritmos compactos e rápidos, adaptados ao uso da linguagem escrita.

Os algoritmos para implementação da subtração em sistemas posicionais tiveram sua gênese na manipulação do ábaco. Para subtrair dois números naturais em um ábaco é suficiente realizar os movimentos opostos àqueles que são feitos na adição.

Vejamos dois exemplos. No primeiro fazemos $56 - 35$. A figura abaixo representa três movimentos desse cálculo.




Nessa figura, no ábaco da esquerda, vemos representado o número 56. No ábaco do meio vemos que da primeira casa foram retiradas 5 pedrinhas, e restou uma, correspondendo ao cálculo $6 - 5 = 1$, realizado na casa das unidades. No ábaco da direita vemos que foram retiradas 3 pedrinhas da segunda casa, correspondendo ao cálculo $5 - 3 = 2$, realizado na casa das dezenas. O resultado é $56 - 35 = 21$.

Na linguagem escrita esses movimentos podem ser indicados por

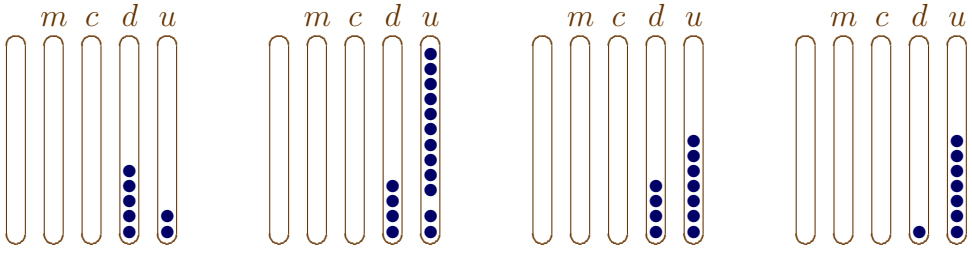
$$\begin{array}{r} 5\,6 \\ -\,3\,5 \\ \hline \end{array} \longrightarrow \begin{array}{r} 5\,6 \\ -\,3\,5 \\ \hline 1 \end{array} \longrightarrow \begin{array}{r} 5\,6 \\ -\,3\,5 \\ \hline 2\,1 \end{array}$$

Podemos sintetizar na forma usual

$$\begin{array}{r} 5\,6 \\ -\,3\,5 \\ \hline 2\,1 \end{array}$$

O exemplo abaixo, em que fazemos $52 - 35$, é mais significativo, pois surge uma situação de *empréstimo*. Embora 52 tenha mais unidades do que 35, na casa das unidades ocorre o contrário.

A figura abaixo representa quatro movimentos desse cálculo. No ábaco da esquerda está representado o número 52. No segundo ábaco vemos o empréstimo: uma pedrinha da casa das dezenas de 52 é emprestada para a casa das unidades, transformando-se em 10 pedrinhas. Portanto a casa das unidades fica provisoriamente com 12 pedrinhas, e a casa das dezenas com quatro. No terceiro ábaco vemos o cálculo $12 - 5 = 7$ feito na primeira casa. Finalmente no quarto ábaco vemos $4 - 3 = 1$ feito na segunda casa. O resultado é $52 - 35 = 17$.




Na linguagem escrita esses movimentos podem ser indicados por

$$\begin{array}{r} 5\,2 \\ -\,3\,5 \\ \hline \end{array} \longrightarrow \begin{array}{r} 4\,(12) \\ -\,3\;\;5 \\ \hline \end{array} \longrightarrow \begin{array}{r} 4\,(12) \\ -\,3\;\;5 \\ \hline 7 \end{array} \longrightarrow \begin{array}{r} 4\,(12) \\ -\,3\;\;5 \\ \hline 1\;\;7 \end{array}$$

Podemos sintetizar na seguinte forma:

$$\begin{array}{r} 4 \\ \not{5}\;{}^{1}2 \\ -\,3\;\;5 \\ \hline 1\;\;7 \end{array}$$

Uma variação desse método usa o recurso da *compensação*:

$$\begin{array}{r} 52 \\ -35 \\ \hline \end{array} \longrightarrow \begin{array}{r} 5\,(12) \\ -4\ \ 5 \\ \hline \end{array} \longrightarrow \begin{array}{r} 5\,(12) \\ -4\ \ 5 \\ \hline 7 \end{array} \longrightarrow \begin{array}{r} 5\,(12) \\ -4\ \ 5 \\ \hline 1\ \ 7 \end{array}$$

Observamos que as subtrações feitas em uma coluna, como $12-5=7$, podem ser calculadas "contando-se nos dedos", como fazem as crianças. Esse é o método da *complementação*, às vezes também denominado *método austríaco*. Pode-se também calcular: $10-5=5$, $5+2=7$. Outra forma é utilizar a tábua de adição do sistema decimal, que em geral é memorizada.

Na operação de subtração se usa a seguinte nomenclatura:

$$\begin{array}{rl} 7 & \longleftarrow \text{ minuendo} \\ -5 & \longleftarrow \text{ subtraendo} \\ \hline 2 & \longleftarrow \text{ diferença ou resto.} \end{array}$$

A subtração pode ser feita da esquerda para a direita, de acordo com os exemplos que seguem. No segundo dispositivo abaixo, a diferença é colocada acima do minuendo, um antigo costume hindu.

$$\begin{array}{r} 425 \\ -249 \\ \hline 2\not{8}6 \\ 17 \end{array} \qquad\qquad \begin{array}{r} 17 \\ \not{2}\not{8}6 \\ 425 \\ 249 \end{array}$$

O resultado dessas subtrações é 176.

Os hindus também usavam outra forma. Veja abaixo como era feito $43826-5349=38477$. O minuendo era escrito abaixo do subtraendo.

$$\begin{array}{r} 1\ \ 11 \\ \hline 5349 \\ 43826 \\ \hline 38477 \end{array}$$

Os estudantes vivem inventando métodos de subtração que evitam o uso do empréstimo. Eis um exemplo esperto:

$$\begin{array}{rl} 43 & (+2) \\ -28 & (+2) \\ \hline \end{array} \longrightarrow \begin{array}{r} 45 \\ -30 \\ \hline 15 \end{array}$$

Outro exemplo, ainda mais esperto:

$$\begin{array}{r} 627 \\ -378 \\ \hline \end{array} \longrightarrow \begin{array}{r} 629 \\ -380 \\ \hline 9 \end{array} \longrightarrow \begin{array}{r} 649 \\ -400 \\ \hline 249 \end{array}$$

O método abaixo permite fazer subtrações usando quase que apenas adições. Para calcular $719-281$ observamos que é o número que, adicionado a 281, resulta 719. Assim

$$\begin{array}{rl} 281 + \phantom{4}9 = 290 & \\ 290 + \phantom{4}10 = 300 & \\ 300 + 400 = 700 & \text{Resposta: } 719 - 281 = 438. \\ 700 + \phantom{4}19 = 719 & \\ \hline \phantom{700 + 1}438 & \end{array}$$

Outro método. Para calcular $719 - 281$ observamos que é o número que, subtraído de 719, resulta 281. Assim

$$\begin{array}{rl} 719 - \phantom{4}9 = 710 & \\ 710 - \phantom{4}10 = 700 & \\ 700 - 400 = 300 & \\ 300 - \phantom{4}10 = 290 & \text{Resposta: } 719 - 281 = 438. \\ 290 - \phantom{4}9 = 281 & \\ \hline \phantom{700 + 1}438 & \end{array}$$

Podemos fazer contas de subtração em um sistema posicional de base qualquer usando o algoritmo usual. Por exemplo, de posse da tábua de adição na base cinco, fica fácil calcular $423 - 242$ nessa base:

| $+_{cinco}$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 |
| 1 | 1 | 2 | 3 | 4 | 10 |
| 2 | 2 | 3 | 4 | 10 | 11 |
| 3 | 3 | 4 | 10 | 11 | 12 |
| 4 | 4 | 10 | 11 | 12 | 13 |

$$\begin{array}{r} \phantom{-}\overset{3}{\not 4}\,\overset{1}{}2\ \ 3 \\ -\ 2\ \ 4\ \ 2 \\ \hline \phantom{-}\ 1\ \ 3\ \ 1 \end{array}_{cinco}$$

### 3.3.3 Problemas

**Problema 3.3.3.1.** Sejam $a$, $b$ e $c$ números naturais tais que $b+c$ tem menos unidades do que $a$. Demonstre que

$$(a-b)-c = (a-c)-b. \tag{3.10}$$

**Problema 3.3.3.2.** Sejam $a$, $b$ e $c$ números naturais tais que $b$ tem menos unidades do que $a$. Demonstre que

$$a-(b-c) = (a-b)+c = (a+c)-b. \tag{3.11}$$

**Problema 3.3.3.3.** Sejam $a$, $b$ e $c$ números naturais tais que $c$ tem menos unidades do que $a$ e do que $b$. Demonstre que

$$(a-c)+(b-c) = [(a+b)-c]-c. \tag{3.12}$$

**Problema 3.3.3.4.** Sejam $a$, $b$ e $c$ números naturais tais que $b+c$ tem menos unidades do que $a$. Demonstre que

$$a-(b+c) = (a-b)-c. \tag{3.13}$$

**Problema 3.3.3.5.** Sejam $a$, $b$ e $c$ números naturais tais que $b+c$ tem menos unidades do que $a$. Demonstre que

$$(a-b)-(a-c) = c-b. \tag{3.14}$$

**Problema 3.3.3.6.** Efetue DCCXLIX−CCLXXIII no sistema romano.

**Problema 3.3.3.7.** Descreva como se pode efetuar $8342 - 2659$ no ábaco da Figura 3.1.

**Problema 3.3.3.8.** Veja se é legal:

$$\begin{array}{r} 323 \\ -139 \\ \hline \end{array} \rightarrow \begin{array}{r} 320 \\ -136 \\ \hline \end{array} \rightarrow \begin{array}{r} 220 \\ -36 \\ \hline \end{array} \rightarrow \begin{array}{r} 200 \\ -16 \\ \hline \end{array} \rightarrow \begin{array}{r} 190 \\ -\ 6 \\ \hline 184 \end{array}$$

**Problema 3.3.3.9.** Efetue na base indicada:

$$(450521)_{seis} - (354045)_{seis}\ ;$$

$$(63102)_{sete} - (4256)_{sete}\ ;$$

$$(73012)_{oito} - (10663)_{oito}\ ;$$

$$(1011100)_{dois} - (100111)_{dois}\ .$$

**Problema 3.3.3.10.** Efetue $(6035)_{oito} - (5276)_{oito}$ usando o algoritmo usual, mas iniciando da coluna da esquerda.

**Problema 3.3.3.11.** Descreva uma "regra do antecessor" para o sistema decimal, de forma análoga à regra do sucessor descrita no texto (página 26). Faça o mesmo para um sistema posicional qualquer.

**Problema 3.3.3.12.** Encontre a representação binária dos números $2^{n-1}(2^n - 1)$ para todo número natural $n$.

**Problema 3.3.3.13.** Eis um método de subtração que é utilizado em máquinas mecânicas de calcular. Uma máquina de calcular lida com uma quantidade finita de números, e tem um número máximo, digamos 9999. Dessa forma, a máquina conta de 0000 a 9999, e o número seguinte é novamente 0000. Dado um número natural $a$, o complemento de $a$ é o número $c(a) = 10000 - a$, isto é, é o número que falta para que, a partir de $a$, o mostrador mecânico da máquina atinja a marca 0000. O mecanismo da máquina "sabe" o complemento de qualquer número. A subtração é então reduzida à adição:

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

Verifique essa fórmula.

**Problema 3.3.3.14.** Um estudante inventou seu próprio método de efetuar a subtração. Eis um exemplo:

$$\begin{array}{r} 54 \\ -26 \\ \hline \end{array} \qquad \begin{array}{l} \text{1) Faça } \ 6 - 4 = 2; \\ \text{2) Faça } \ 50 - 20 = 30; \\ \text{3) O resto procurado é } \ 30 - 2 = 28. \end{array}$$

**a)** Explique em que circunstâncias e por que funciona o método do estudante.

**b)** Tente imaginar por que o estudante teria inventado esse método, o que ele facilita em relação ao método usual.

**c)** Quais são as desvantagens desse método em relação ao método usual, e por qual motivo esse método não é ensinado nas escolas no lugar do método usual.

**Problema 3.3.3.15.** Ao efetuar $4738 - 3912$, um estudante fez o seguinte. Primeiro substituiu cada dígito do subtraendo pelo seu complemento relativamente a nove, obtendo o número 6087. Depois adicionou 4738 ao número assim obtido, da seguinte forma:

$$\begin{array}{r} 4\,7\,3\,8 \\ +\,6\,0\,8\,7 \\ \hline 1\!\!\not{1}\,0\,8\,2\,5 \\ \hookrightarrow \quad +1 \\ \hline 8\,2\,6 \end{array}$$

Então, concluiu, $4738 - 3912 = 826$.

**a)** Explique por que esse método funciona com números com a mesma quantidade de dígitos. Investigue se esse método funciona quaisquer que sejam os números envolvidos.

**b)** Efetue na base dois, usando o mesmo método:

$$(1\,011\,001)_{dois} - (110\,111)_{dois}\,.$$

**c)** Efetue na base oito:

$$(73265)_{oito} - (32156)_{oito}\,.$$

## 3.4 Ordenação dos números naturais

Existe uma ordem no conjunto dos números naturais. Dados números naturais $a$ e $b$, podemos compará-los e verificar se têm a mesma quantidade de unidades, ou se um deles tem uma quantidade maior do que a do outro.

Como já sabemos, escrevemos $a = b$ (e lemos $a$ igual a $b$) para expressar que os símbolos $a$ e $b$ indicam o mesmo número natural, isto é, têm a mesma quantidade de unidades.

Se $a$ tem mais unidades do que $b$, escrevemos $a > b$, ou $b < a$, e dizemos $a$ maior do que $b$, ou, respectivamente, $b$ menor do que $a$.

São muito úteis as seguintes notações: dados $a$ e $b$ números naturais, anotamos $a \leq b$ quando $a = b$ ou $a < b$ (lê-se $a$ menor ou igual a $b$). Da mesma forma, anotamos $a \geq b$ quando $a = b$ ou $a > b$ (lê-se $a$ maior ou igual a $b$).

Notemos que se $a$ tem menos unidades do que $b$ e se este tem menos unidades do que $c$, então $a$ tem menos unidades do que $c$. Temos assim a

*propriedade transitiva da ordem*: quaisquer que sejam os números naturais $a$, $b$ e $c$, se $a < b$ e $b < c$, então $a < c$.

Notemos ainda que, dados números $a$ e $b$, ou eles têm a mesma quantidade de unidades, ou um deles tem maior quantidade do que a do outro. Destacamos essa observação na

*Lei da Tricotomia*: dados números naturais $a$ e $b$, uma e apenas uma das seguintes condições é verdadeira: *i)* $a = b$; *ii)* $a < b$; *iii)* $a > b$.

Temos ainda a destacar:

*Princípio do Menor Número Natural:* se $A$ é um subconjunto não vazio do conjunto dos números naturais, então $A$ tem um menor elemento. Isso significa que existe $a \in A$ tal que $a < b$ para todo $b$ em $A - \{a\}$.

Faremos comentários sobre essa propriedade no Capítulo 9, Seção 9.5.

Observamos a seguinte propriedade de compatibilidade entre a ordem e a adição:

*compatibilidade entre a ordem e a adição*: quaisquer que sejam os números naturais $a$, $b$ e $c$, se $a < b$ então $a + c < b + c$. Temos também: se $a \leq b$ então $a + c \leq b + c$.

De fato, se $b$ tem mais unidades do que $a$, e se adicionarmos a cada um a mesma quantidade $c$ de unidades, então $b + c$ tem mais unidades do que $a + c$. Por outro lado, se $a = b$ então $a + c = b + c$, pois estamos somando $c$ ao mesmo número. Com isso vale a segunda afirmação.

**Problema resolvido 3.1.** Quaisquer que sejam os números naturais $a$, $b$, $c$ e $d$, se $a < b$ e $c < d$, então $a + c < b + d$.

*Solução.* Aplicamos a propriedade compatibilidade entre a ordem e a adição duas vezes. De $a < b$ vem $a + c < b + c$. De $c < d$ vem $c + b < d + b$. Em virtude da transitividade da ordem segue que $a + c < b + d$. □

### 3.4.1 Problemas

**Problema 3.4.1.1.** Verifique se é verdadeira ou falsa cada uma das afirmações abaixo, e justifique. **a)** $2 \leq 3$. **b)** se $a$, $b$ e $c$ são números naturais tais que $a \leq b$ e $b < c$, então $a < c$. **c)** se $a$, $b$ e $c$ são números naturais tais que $a < b$ e $b \leq c$, então $a < c$. **d)** se $a$, $b$ e $c$ são números naturais tais que $a \leq b$ e $b \leq c$, então $a \leq c$.

**Problema 3.4.1.2.** Qual é a negativa das seguintes afirmações, em que $a$, $b$, $c$ e $d$ são números naturais: **a)** $a \leq b$; **b)** $c > d$.

**Problema 3.4.1.3.** Estude variações das propriedades da ordem. Por exemplo, se $a \leq b$ e $c < d$, então $a + c < b + d$.

**Problema 3.4.1.4.** Demonstre que $a + 1 \leq b$ se e somente se $a < b$, quaisquer que sejam os números naturais $a$ e $b$. Prove também que $a + 1 > b$ se e somente se $a \geq b$.

**Problema 3.4.1.5.** (Lei de Cancelamento da ordem em relação à adição) Sejam $a$, $b$ e $c$ números naturais tais que $a + c < b + c$. Demonstre que $a < b$. E se $a + c \leq b + c$ ?

**Problema 3.4.1.6.** Demonstre que, quaisquer que sejam os números naturais $a$ e $b$, temos $b < a$ se e somente se existe um número natural $c$ tal que $a = b + c$.

**Problema 3.4.1.7.** Vale uma Lei do Cancelamento da ordem em relação à subtração? Isto é, $a - c < b - c \Rightarrow a < b$ ? Enuncie corretamente uma propriedade e justifique.

**Problema 3.4.1.8.** Vale a compatibilidade da ordem em relação à subtração? Isto é, $a < b \Rightarrow a - c < b - c$ ? Enuncie corretamente uma propriedade e justifique.

**Problema 3.4.1.9.** Sejam $a$, $b$ e $c$ números naturais tais que $c$ tem menos unidades do que $a$. Demonstre que $a < b + c \Rightarrow a - c < b$.

*Solução:* Notemos primeiro que $a < b + c$ implica que $c$ tem menos unidades do que $a$, de modo que existe $a - c$. Por (3.2) temos $a = (a - c) + c$, logo $(a - c) + c < b + c$. Pela Lei do Cancelamento da ordem em relação à adição (Problema 3.4.1.5) vem $a - c < b$.

**Problema 3.4.1.10.** Demonstre que, quaisquer que sejam os números naturais $a$, $b$ e $c$, sendo que $c$ tem menos unidades do que $b$, temos $a < b - c \Rightarrow a + c < b$.

**Problema 3.4.1.11.** Demonstre que, quaisquer que sejam os números naturais $a$, $b$ e $c$ tais que $b$ e $c$ têm menos unidades do que $a$, temos $a - b < a - c \Rightarrow c < b$.

*Solução:* Temos $a - b < a - c \Rightarrow (a - b) + b < (a - c) + b$ (compatibilidade entre a ordem e a adição, página 67) $\Rightarrow a < (a - c) + b$ (por (3.2)) $\Rightarrow a < (a + b) - c$ (por (3.7)) $\Rightarrow a + c < a + b$ (por Problema 3.4.1.10) $\Rightarrow c < b$ (por cancelamento Problema 3.4.1.5)

**Problema 3.4.1.12.** Demonstre que se $a = (a_m \dots a_1 a_0)_\beta$ e $b = (b_n \dots b_1 b_0)_\beta$ são números naturais representados na base $\beta \geq 2$, com $m > n$, $a_m \neq 0$ e $b_n \neq 0$, então $a > b$.

**Problema 3.4.1.13.** Sejam $a = (a_m \dots a_1 a_0)_\beta$ e $b = (b_m \dots b_1 b_0)_\beta$ números naturais representados na base $\beta \geq 2$. Descreva condições suficientes sobre os dígitos de $a$ e $b$ para que $a > b$.

**Problema 3.4.1.14.** Você está convencido de todas as afirmações feitas nesta Seção? E quanto ao Princípio do Menor Número Natural? Redija uma justificativa. Não se esqueça de considerar que o conjunto $A$ pode ser infinito.

## 3.5 A multiplicação

A multiplicação é um caso especial da adição, em que são somadas parcelas iguais. O estudo em separado desse caso de adição nos permite potencializar seu uso.

### 3.5.1 Conceito de multiplicação

*Duplicar* um número natural significa adicionar duas parcelas iguais a esse número. Assim, o *dobro* de $a$ é $a + a$. *Triplicar* um número significa adicionar três parcelas iguais a esse número. Assim o *triplo* de $a$ é $a + a + a$. Continuando, temos *quadruplicar*, *quintuplicar*, em geral, *multiplicar*.

Multiplicar um número natural $a$ por um número natural $n$ significa adicionar $n$ parcelas iguais a $a$. O resultado se chama *produto de $n$ por $a$* e é indicado com uma das seguintes notações:

$$na\,, \qquad n \cdot a \qquad \text{ou} \qquad n \times a\,.$$

(lê-se: n vezes a, ou n multiplicado por a). Nesse contexto entende-se que $1 \cdot a = a$.

A multiplicação ocorre em inúmeras situações, como contagem de objetos colocados em um arranjo retangular ou no cálculo da medida da área de um retângulo de base $a$ e altura $b$, sendo $a$ e $b$ números naturais, por contagem de quadrados unitários.

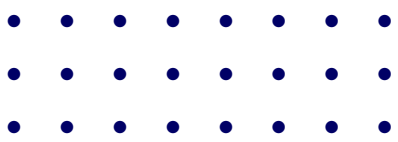


Figura 3.2. Representação das unidades de $3 \cdot 8$.

Para calcular um produto como $3 \cdot 8$ podemos organizar as unidades de 8, fazendo 3 fileiras delas. Representando essas unidades por pontos, e organizando-os em forma de matriz, obtemos a situação da Figura 3.2. Assim, contando os pontos fila a fila, temos $3 \cdot 8 = 8 + 8 + 8 = 24$.

Mas esses pontos podem também serem contados coluna a coluna, de modo que $3 \cdot 8 = 3+3+3+3+3+3+3+3 = 24$.

Considerando esse mesmo esquema para números naturais quaisquer $a$ e $b$, temos a

*Comutatividade da multiplicação*: $ab = ba$ quaisquer que sejam os números naturais $a$ e $b$.

Vejamos outra propriedade. Dados números naturais $a$, $b$ e $c$, consideremos dois arranjos retangulares de pontos, o primeiro com $b$ colunas, o segundo com $c$ colunas, e ambos com $a$ linhas. O primeiro representa as unidades de $ab$, e o segundo, as de $ac$. Considerados em conjunto, representam as unidades de $ab + ac$. A Figura 3.3, à esquerda, mostra esses dois arranjos.

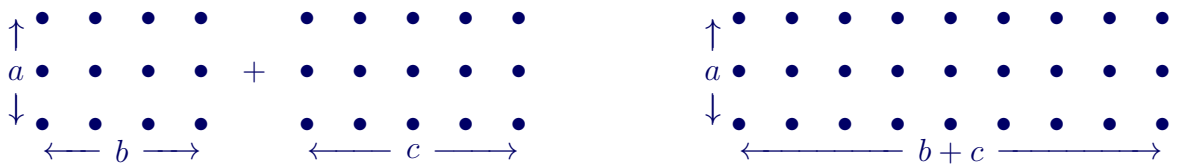



Figura 3.3. À esquerda, representação das unidades de $ab + ac$. À direita, representação das unidades de $a(b + c)$.

Juntando agora os dois arranjos para formar um único retângulo (Figura 3.3 à direita), contamos $a(b + c)$ unidades. Isso ilustra a propriedade

*propriedade distributiva da multiplicação em relação à adição*: quaisquer que sejam os números naturais $a$, $b$ e $c$, temos $a(b + c) = ab + ac$.

Sejam $a$, $b$ e $c$ números naturais quaisquer. Consideremos um arranjo de pontos em forma de paralelepípedo reto retângulo, com dimensões $a$, $b$ e $c$. Podemos contar os pontos desse arranjo de várias formas, por exemplo, começando com a face de lados $b$ e $c$. Dessa contagem resulta $bc$. Somando esse valor $a$ vezes, contamos todos os pontos, e resulta $a(bc)$. De outra forma, contamos os pontos da face de lados $a$ e $b$, do que resulta $ab$, e depois somamos esse valor $c$ vezes, do que resulta $(ab)c$. Naturalmente o resultado é o mesmo. Temos assim a

*Associatividade da multiplicação*: quaisquer que sejam os números naturais $a$, $b$ e $c$, temos $a(bc) = (ab)c$.

Sejam $a$ e $b$ números naturais tais que $a < b$. Aplicando a propriedade 3.1 a $a < b$ e a $a < b$ vem $a+a < b+b$, ou $2a < 2b$. Juntando essa última com $a < b$ novamente, vem $2a+a < 2b+b$, ou $3a < 3b$. E assim sucessivamente, se $a < b$ então $na < nb$ qualquer que seja o número natural $n$. Assim obtemos a

*compatibilidade entre a ordem e a multiplicação*: quaisquer que sejam os números naturais $a$, $b$ e $n$, se $a < b$ então $an < bn$. Temos também: se $a \leq b$ então $an \leq bn$.

**Problema resolvido 3.2.** (*Leis de Cancelamento da multiplicação*) (i) Quaisquer que sejam os números naturais $a$, $b$ e $n$, se $na < nb$ então $a < b$. (ii) Quaisquer que sejam os números naturais $a$, $b$ e $n$, se $na = nb$ então $a = b$.

*Solução.* (i) Sobre os números $a$ e $b$ podemos afirmar que $a = b$ ou $a > b$ ou $a < b$. Se fosse $a = b$ teríamos $na = nb$, o que não é o caso. Se fosse $a > b$ teríamos, pela compatibilidade entre a ordem e a multiplicação demonstrada acima, que $na > nb$, o que também não é o caso. Resta a possibilidade $a < b$, que é a que queríamos. (ii) Por argumento análogo. □

### 3.5.2 Algoritmos para a multiplicação

O método mais básico que podemos usar para multiplicar dois números consiste em aplicar a definição. Assim, para calcular $5 \times 12$ basta fazer a adição $12 + 12 + 12 + 12 + 12 = 60$.

Certamente que não gostaríamos de utilizar esse método para números maiores, por exemplo, $35 \times 273$. Para aplicar a multiplicação nas mais variadas situações necessitamos de um algoritmo que traga economia de tempo e esforço, e seja adaptado para uso em linguagem escrita. Esse é sem dúvida o algoritmo usual, que aprendemos nas escolas. Vejamos a gênese desse algoritmo.

Começamos observando, como uma ideia inicial, que para calcular $35 \times 273$ não necessitamos somar $273 + \ldots + 273$ (35 vezes). De fato, $273 + 273 = 546$, e não necessitamos mais repetir essa soma. Podemos mesmo aproveitá-la, fazendo $546 + 546 = 1092$, de forma que $4 \times 273 = 1092$. Agora $1092 + 1092 = 2184$ nos fornece $8 \times 273 = 2184$. E assim por diante, obtemos $16 \times 273 = 4368$ e $32 \times 273 = 8736$. Como $35 = 32 + 2 + 1$, temos $35 \times 273 = 32 \times 273 + 2 \times 273 + 273 = 8736 + 546 + 273 = 9555$.

Vimos que conseguimos economizar um bocado de contas. Mas podemos economizar mais. A ideia acima usa a duplicação. Mas, como estamos representando os números no sistema decimal, certamente será melhor usarmos a decuplicação. Observamos que o efeito de multiplicar um número por 10 é o deslocamento de seus dígitos uma casa acima. Assim, $10 \times 273 = 2730$, e o dígito 3, que estava na primeira casa, vai para a segunda, o dígito 7, que estava na segunda casa, vai para a terceira, e assim por diante.

Isso ocorre visto que

$$\begin{aligned} 10 \times 273 &= 10 \times (2 \times 10^2 + 7 \times 10 + 3) \\ &= 2 \times 10^3 + 7 \times 10^2 + 3 \times 10 \\ &= 2730. \end{aligned}$$

Em geral, quando multiplicamos por $10^n$ o número $a = a_m 10^m + \ldots a_1 10 + a_0$, cada dígito $a_i$ é deslocado $n$ casas para a esquerda, e as primeiras $n$ casas de $10^n a$ são ocupadas por zeros.

Essa observação pode ser usada para o cálculo de $35 \times 273$. Notando que $35 = 3 \times 10 + 5$, temos $35 \times 273 = (3 \times 10 + 5)273 = 3 \times 10 \times 273 + 5 \times 273 = 3 \times 2730 + 5 \times 273$. Para completar fazemos agora os cálculos $3 \times 2730 = 2730 + 2730 + 2730 = 8190$ e $5 \times 273 = 1365$, e temos $35 \times 273 = 8190 + 1365 = 9555$.

Observando esses cálculos vemos que necessitamos de um método melhor para multiplicar um número natural qualquer por um número de um dígito.

Por exemplo, precisamos descobrir um método de sintetizar o cálculo

$$\begin{array}{r} {\scriptstyle 3\ \ 1\ \ \ } \\ 2\,7\,3 \\ 2\,7\,3 \\ +\ 2\,7\,3 \\ 2\,7\,3 \\ 2\,7\,3 \\ \hline 1\,3\,6\,5 \end{array}$$

Inicialmente observamos que não há necessidade de repetir 273. Basta escrevê-lo uma vez. Embaixo dele colocamos 5 para lembrar que estamos multiplicando por 5.

$$\begin{array}{r} 2\,7\,3 \\ \times\quad 5 \\ \hline \end{array}$$

A seguir implementamos o cálculo como se estivéssemos fazendo a soma acima. Tomamos o dígito 3 de 273 e calculamos $5 \times 3 = 3 + 3 + 3 + 3 + 3 = 15$. Escrevemos 5 na primeira coluna

e reservamos 1 na coluna seguinte. E assim sucessivamente, obtemos $5 \times 273 = 1365$.

$$\begin{array}{r} {\scriptstyle 3\ 1\ \ } \\ 2\,7\,3 \\ \times \quad 5 \\ \hline 1\,3\,6\,5 \end{array}$$

Nesse estágio de nosso estudo percebemos como é importante termos na memória os produtos de dois algarismos quaisquer. Por isso é que nossos professores das séries iniciais sempre insistiram em que memorizássemos a tabuada da multiplicação.

Temos agora todos os ingredientes para implementar $35 \times 273$ de forma sintética. Podemos acompanhar abaixo os passos principais.

$$\begin{array}{r} 2\,7\,3 \\ \times \quad 3\,5 \\ \hline \end{array} \rightarrow \begin{array}{r} {\scriptstyle 3\ 1\ \ } \\ 2\,7\,3 \\ \times \quad 3\,5 \\ \hline 1\,3\,6\,5 \end{array} \rightarrow \begin{array}{r} {\scriptstyle 2\ \ \ } \\ {\scriptstyle 3\ 1\ \ } \\ 2\,7\,3 \\ \times \quad 3\,5 \\ \hline 1\,3\,6\,5 \\ 8\,1\,9\,0 \end{array} \rightarrow \begin{array}{r} {\scriptstyle 2\ \ \ } \\ {\scriptstyle 3\ 1\ \ } \\ 2\,7\,3 \\ \times \quad 3\,5 \\ \hline 1\,3\,6\,5 \\ +\,8\,1\,9\,0 \\ \hline 9\,5\,5\,5 \end{array}$$

Podemos reconhecer nesses cálculos um dispositivo prático para implementar o seguinte esquema:

$$\begin{aligned} 35 \times 273 &= (3 \times 10 + 5)273 \\ &= 3 \times 273 \times 10 + 5 \times 273 \\ &= 8\,190 + 1\,365 \\ &= 9\,555. \end{aligned}$$

Com a prática omitimos as reservas assim como os zeros originados de deslocamentos. Por exemplo,

$$\begin{array}{r} 1\,2\,3 \\ \times 3\,4\,5 \\ \hline 6\,1\,5 \\ 4\,9\,2 \\ 3\,6\,9 \\ \hline 4\,2\,4\,3\,5 \end{array}$$

Pensamos que esses exemplos esclarecem a gênese do algoritmo usual da multiplicação.

Na multiplicação usamos a seguinte nomenclatura:

$$\begin{array}{r} 3 \\ \times 5 \\ \hline 1\ 5 \end{array} \begin{array}{l} \\ \longrightarrow \text{fatores} \\ \\ \longrightarrow \text{produto} \end{array} \qquad \text{ou} \qquad \begin{array}{r} 3 \\ \times 5 \\ \hline 1\ 5 \end{array} \begin{array}{l} \longrightarrow \text{multiplicando} \\ \longrightarrow \text{multiplicador} \\ \longrightarrow \text{produto} \end{array}$$

Pode ter interesse pedagógico o chamado *método longo*, conforme o exemplo seguinte:

$$\begin{array}{r} 7\,6 \\ \times 3\,9 \\ \hline 5\,4 \\ 6\,3 \\ 1\,8 \\ 2\,1 \\ \hline 2\,9\,6\,4 \end{array}$$

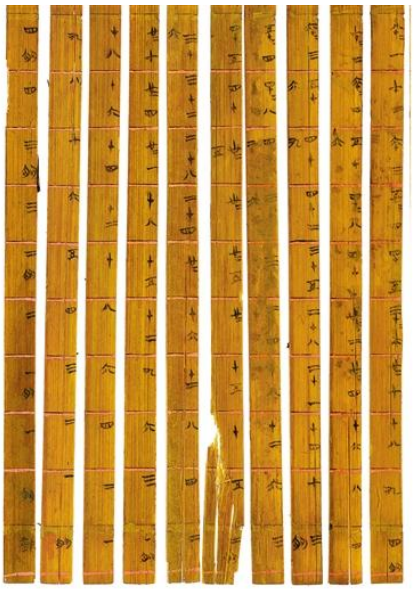


Figura 3.4. Antiga tábua de multiplicação chinesa feita com tiras de bambu, datada de 446-221 a.C. Faz parte do acervo da Universidade de Tsinghua. Acredita-se que seja o mais antigo artefato conhecido para o cálculo da multiplicação. Mais informações em `https://en.wikipedia.org/wiki/Tsinghua_Bamboo_Slips` Consultado em 26 de setembro de 2016.

O algoritmo de multiplicação comumente usado no sistema decimal é válido para qualquer sistema posicional. Vejamos alguns exemplos na base cinco. Para maior comodidade tenhamos à mão a tábua de multiplicação nessa base.

| $\times_{cinco}$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 |
| 2 | 0 | 2 | 4 | 11 | 13 |
| 3 | 0 | 3 | 11 | 14 | 22 |
| 4 | 0 | 4 | 13 | 22 | 31 |

Vejamos agora os exemplos.

$$\begin{array}{r} 3\,2\,1\,4 \\ \times\quad\;\; 4 \\ \hline \end{array}_{cinco}$$
$$\begin{array}{r} \quad\;\; 3\;1 \\ \quad\;\; 4 \\ 1\;3 \\ 2\;2 \\ \hline \end{array}_{cinco}$$
$$2\;3\;4\;2\;1$$

$$\begin{array}{r} {\scriptstyle 1\;\;1\;\;3} \\ 3\,2\,1\,4 \\ \times\quad\;\; 4 \\ \hline \end{array}_{cinco}$$
$$2\;3\;4\;2\;1$$

$$\begin{array}{r} 3\;4\;1 \\ \times 2\;3 \\ \hline \end{array}_{cinco}$$
$$\begin{array}{r} 2\;1\;2\;3 \\ 1\;2\;3\;2 \\ \hline \end{array}_{cinco}$$
$$1\;4\;4\;4\;3$$

O antigo método de multiplicação egípcio tem interesse histórico. Utiliza o método da duplicação, já comentado no início desta seção. Não depende do sistema de numeração, e pode ser aplicado a sistemas não posicionais. Devido a esse fato foi muito utilizado no mundo antigo.

Vamos exemplificar multiplicando 6 por 13. Começamos dispondo duas colunas. Na primeira colocamos potências de dois: 1, 2, 4, 8, etc., de modo que o último número não ultrapasse o valor de um dos fatores, previamente escolhido. Assim, escolhendo o fator 13, o último número da primeira coluna deve ser 8. Na segunda coluna, dispomos o outro fator, no caso 6, e o duplicamos sucessivamente, conforme se mostra abaixo, à esquerda.

À direita podemos ver como se finaliza o cálculo. Usando tentativa e erro observamos que $13 = 1 + 4 + 8$ (essa é a decomposição de 13 em potências de 2). Assinalamos com * as linhas que correspondem aos números 1, 4 e 8. Somamos os números da segunda coluna que constam

das linhas assinaladas: $6 + 24 + 48 = 78$. Esse é o produto procurado.

| | |
|---|---|
| 1 | 6 |
| 2 | 12 |
| 4 | 24 |
| 8 | 48 |

| | | |
|---|---|---|
| $*$ | 1 | 6 |
| | 2 | 12 |
| $*$ | 4 | 24 |
| $*$ | 8 | 48 |
| Totais | 13 | 78 |

Para justificar o método egípcio consideremos números naturais $a$ e $b$. Seja $a = 2^n + a_{n-1}2^{n-1} + \cdots + a_1 2 + a_0$ a expansão de $a$ no sistema binário. Notemos que $2^n$ é a maior potência de 2 que não ultrapassa $a$, e os coeficientes $a_i$ podem ser 1 ou 0. Se $a_i = 1$, então a potência $2^i$ comparece na expansão binária de $a$. Se $a_i = 0$, a potência $2^i$ não comparece. Vejamos agora que $a \cdot b = (2^n b) + a_{n-1}(2^{n-1}b) + \cdots + a_1(2b) + a_0(b)$ e os termos que aí comparecem são aqueles que correspondem aos termos $a_i \neq 0$. Esses termos são aqueles cujas linhas são assinaladas por * na seguinte disposição:

| | |
|---|---|
| 1 | $b$ |
| 2 | $2b$ |
| 4 | $4b$ |
| $\vdots$ | $\vdots$ |
| $2^n$ | $2^n b$ |
| $a$ | $a \cdot b$ |

Terminamos a justificativa do método egípcio de multiplicação.

Diversos dispositivos de multiplicação para o sistema decimal foram desenvolvidos pelos hindus, e são descritos em obras como *Lilavati*, escrita por Bhaskara por volta do ano de 1150. Esses métodos foram adotados em diversas obras européias sobre aritmética do Século XV.

Apresentamos brevemente alguns desses dispositivos, através de exemplos. Outros métodos são propostos como problemas.

Cálculo de $13 \cdot 217$; o resultado é 2821:

| | | | |
|---|---|---|---|
| | 2 | 1 | 7 |
| $\times$ | 1 | 3 | |
| 2 | 6 | | |
| | 1 | 3 | |
| | | 9 | 1 |
| 2 | 8 | 2 | 1 |

Variação do método anterior:

| | | | |
|---|---|---|---|
| | 2 | 1 | 7 |
| $\times$ | 1 | 3 | |
| | 2 | 1 | 7 |
| | | 6 | 5 | 1 |
| 2 | 8 | 2 | 1 |

Cálculo de $35 \cdot 46$; o resultado é 1610:

| | | | | |
|---|---|---|---|---|
| | | | | 3 |
| | | | | 5 |
| | | | 4 | 6 |
| | | | 3 | 0 |
| | | 1 | 8 | |
| | | 2 | 0 | |
| | 1 | 2 | | |
| 1 | 6 | 1 | 0 | |

### 3.5.3 Problemas

**Problema 3.5.3.1.** Enuncie corretamente e justifique uma *propriedade distributiva da multiplicação em relação à subtração:*

$$n(a-b) = na - nb.$$

Sugestão: use um esquema similar ao da Figura 3.3.

**Problema 3.5.3.2.** Sejam $a$ e $b$ números naturais tais que $2b$ tem menos unidades do que $a$. Demonstre que

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

*Solução:* Como $2b$ tem menos unidades do que $a$, podemos retirar $b$ unidades de $a$ duas vezes, de forma que $(a-b)-b$ e $a-2b$ estão bem definidos. Seja $m=(a-b)-b$. Temos $m+b=a-b$, e $(m+b)+b=a$. Aplicando a associativa vem $m+(b+b)=a$, e $m+2b=a$. Logo $m=a-2b$, e segue o resultado. Usamos (3.6) três vezes.

**Problema 3.5.3.3.** Sejam $a$, $b$, $c$ e $d$ números naturais. Demonstre que: (i) $(a+b)(c+d) = ac+bc+ad+bd$; (ii) $(a+b)^2 = a^2+2ab+b^2$.

**Problema 3.5.3.4.** Sejam $a$, $b$, $c$ e $d$ números naturais tais que $d$ tem menos unidades do que $c$. Demonstre que $(a+b)(c-d) = [(ac+bc)-ad]-bd$.

*Solução:* $m=(a+b)(c-d) \Rightarrow m=(a+b)c-(a+b)d \Rightarrow m=ac+bc-(ad+bd) \Rightarrow m+(ad+bd)=ac+bc \Rightarrow (m+bd)+ad=ac+bc \Rightarrow m+bd=(ac+bc)-ad \Rightarrow m=[(ac+bc)-ad]-bd$. Como $d$ tem menos unidades do que $c$, todas as subtrações estão bem definidas. Usamos (3.6) e (3.7).

**Problema 3.5.3.5.** Sejam $a$, $b$, $c$ e $d$ números naturais tais que $b$ tem menos unidades do que $a$ e $d$ tem menos unidades do que $c$. Demonstre que $(a-b)(c-d) = [(ac+bd)-bc]-ad$.

**Problema 3.5.3.6.** Sejam $a$ e $b$ números naturais tais que $b$ tem menos unidades do que $a$. Demonstre que $(a-b)^2 = (a^2+b^2)-2ab$.

**Problema 3.5.3.7.** Observe as propriedades de simetria e regularidade em uma tábua de multiplicação. Utilizando essas propriedades construa as tábuas de multiplicação nas bases dois, quatro e sete. Efetue nas bases indicadas usando o algoritmo usual:

$$(1001)_{dois} \times (101)_{dois}\ ;$$

$$(1110011)_{dois} \times (10001101)_{dois}\ ;$$

$$(23103)_{quatro} \times (32)_{quatro}\ ;$$

$$(1030223)_{quatro} \times (323)_{quatro}\ ;$$

$$(4500613)_{sete} \times (302)_{sete}\ .$$

**Problema 3.5.3.8.** Considerando o algoritmo usual de multiplicação, compare os métodos curto e longo, descrevendo as vantagens e desvantagens de um sobre o outro.

**Problema 3.5.3.9.** Se você vivesse na Roma antiga e não conhecesse nenhum sistema de numeração posicional, como calcularia o produto de XXIII por LVII? Como essa tarefa o ajuda na comparação entre os sistemas aditivos e os posicionais?

**Problema 3.5.3.10.** Um estudante calculou $245 \times 12$ assim:

$$\begin{array}{r} {\scriptstyle 5}\ {\scriptstyle 6} \\ 2\ 4\ 5 \\ \times\ 1\ 2 \\ \hline 2\ 9\ 4\ 0 \end{array}$$

Como foi feito esse cálculo? Faça outros exemplos. O que é diferente aqui em relação ao algoritmo usual?

**Problema 3.5.3.11.** No cálculo de multiplicação abaixo ache os dígitos $a$ e $b$, e explique sua estratégia de solução.

$$\begin{array}{r} a\ 2\ a \\ \times\quad a \\ \hline b\ 6\ b \end{array}$$

**Problema 3.5.3.12.** Um antigo método de multiplicar, denominado *método camponês russo*, pode ser exemplificado com o cálculo do produto $25 \cdot 31$:

$$\begin{array}{rr} *25 & 31 \\ 12 & 62 \\ 6 & 124 \\ *3 & 248 \\ *1 & 496 \\ & \overline{775} \end{array}$$

Dessa disposição se conclui que $25 \cdot 31 = 775$. Faça outros exemplos. Explique e justifique o método.

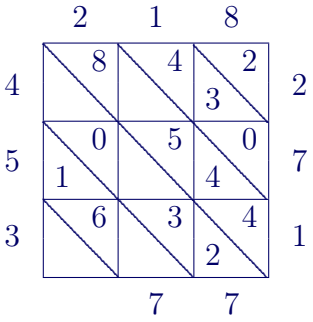
**Problema 3.5.3.13.** Estude esse antigo método hindu. Vemos o cálculo de $327 \cdot 536$. O resultado é 175 272.

$$\begin{array}{rrrrr} & & 3 & 2 & 7 \\ \hline 1 & 9 & 6 & 2 & \diagup\ 6 \\ & 9 & 8 & 1 & \diagup\ 3 \\ 1 & 6 & 3 & 5 & \diagup\ 5 \\ \hline 1 & 7 & 5 & 2 & 7\ 2 \end{array}$$

**Problema 3.5.3.14.** Este é o antigo *método do quadrilátero*. Vemos abaixo o cálculo de $327 \cdot 536$. O resultado é 175 272. Como não é feito o deslocamento correspondente às dezenas, centenas, etc., a soma dos produtos parciais é feita em diagonal, da esquerda para a direita e de cima para baixo. Estude esse método.

$$\begin{array}{rrrrrr} & & 3 & 2 & 7 & \\ \hline 1 & 9 & 6 & 2 & & 6 \\ & 9 & 8 & 1 & & 3 \\ 1 & 6 & 3 & 5 & & 5 \\ \hline 1 & 7 & 5 & 2 & 7 & 2 \end{array}$$

**Problema 3.5.3.15.** Vemos a seguir o produto de $218 \cdot 354$ pelo *método da gelosia*. O resultado é 77172. A soma dos produtos parciais é feita em diagonal. Estude esse método.




**Problema 3.5.3.16.** Para calcular $43 \times 47$ podemos fazer $3 \times 7 = 21$ e $4 \times 5 = 20$ e encadear 21 com 20 obtendo $43 \times 47 = 2021$. O cálculo fica assim:

$$\begin{array}{r} 4\ 7 \\ \times\ 4\ 3 \\ \hline 2\ 0\ 2\ 1 \end{array}$$

Encontre outros exemplos. Explique por que funciona. Veja como aplicar essa ideia para calcular $103 \times 107$.

**Problema 3.5.3.17.** Multiplicando 4 por 2178 encontramos seu reverso 8712. Encontre o número de quatro dígitos que multiplicado por 9 dê o seu reverso. O número que você obteve é o único com essa propriedade?

**Problema 3.5.3.18.** Demonstre que é um número de Fermat o produto

$$(1\,010\,000\,001)_{dois} \times (11\,001\,100\,011\,110\,110\,000\,001)_{dois}\,.$$

Números de Fermat foram definidos no Problema 2.7.17.

## 3.6 A divisão

A divisão amplia o potencial da subtração, e, de certo modo, é inversa da multiplicação. Foi considerada, até o Século XV, uma operação de difícil uso. O autor Luca Pacioli, em sua obra *Suma*, de 1494, diz que "se uma pessoa sabe dividir, tudo o mais é fácil", e consola o estudante discorrendo sobre os benefícios do trabalho pesado. Hoje a divisão é ensinada para crianças, o que deve ser feito com o cuidado necessário.

### 3.6.1 Conceito de divisão

A divisão responde basicamente a dois conceitos: repartir e comparar.

A divisão vista como repartir ocorre quando desejamos particionar um conjunto de objetos em grupos com o mesmo número de objetos cada um, sendo que sabemos a quantidade de grupos e queremos saber a quantidade máxima de objetos que poderão compor cada grupo.

Por exemplo, consideremos o problema de dividir 25 laranjas para 7 estudantes de modo que todos recebam a mesma quantidade de laranjas inteiras. Desse modo queremos dividir 25 laranjas em sete grupos, e precisamos saber quantas laranjas poderá ter cada grupo, sendo essa quantidade a maior possível. Uma estratégia básica é primeiro entregar uma laranja para

cada estudante. Ficamos com $25 - 7 = 18$ laranjas. Entregamos mais uma laranja para cada estudante, e ficamos com $18 - 7 = 11$ laranjas. Repetimos entregando mais uma laranja para cada um, e ficamos com $11 - 7 = 4$. Com as quatro laranjas que sobraram não é possível repartir mais uma vez, de modo que a divisão termina. Dessa forma dividimos 25 em 7 grupos com 3 laranjas cada grupo, e sobram 4 laranjas.

A divisão vista como comparar ocorre quando temos dois números e os comparamos. Queremos saber quantas vezes, no máximo, um número "cabe" no outro. Dizendo de outra forma, dado um conjunto de objetos, queremos organizá-lo em grupos com a mesma quantidade de objetos cada um, sendo que sabemos a quantidade de objetos de cada grupo e queremos saber quantos são os grupos.

Por exemplo, temos 25 laranjas e queremos saber quantos estudantes poderão receber 3 laranjas cada um. Uma estratégia básica consiste em multiplicar 3 por 1, 2, 3,..., até atingir a quantidade máxima que não ultrapassa 25. Temos assim: 1 grupo, $1 \times 3 = 3$ laranjas; dois grupos, $2 \times 3 = 6$ laranjas, e assim por diante, continuamos até chegar a oito grupos, $8 \times 3 = 24$ laranjas. Paramos, pois $25 - 24 = 1$, e 1 não é suficiente para formar outro grupo. Portanto 3 cabe 8 vezes (inteiras) em 25, e sobra 1.

Dado um número natural $a$, suponhamos que $a$ foi dividido em $q$ grupos com $b$ elementos cada um, e que restaram $r$ elementos. Esse fato é representado pela *equação fundamental da divisão*:

$$a = bq + r. \tag{3.15}$$

Um caso especial ocorre se não houver resto. Dizemos então que a divisão é *exata*, e a equação fundamental fica

$$a = bq. \tag{3.16}$$

Nas relações (3.15) e (3.16), $q$ é denominado *quociente* e $r$, *resto* da divisão de $a$ por $b$.

Considerando-se apenas a relação (3.15) o quociente e o resto da divisão de $a$ por $b$ não são únicos. Por exemplo, ao dividir 19 por 3 temos as possibilidades, dentre outras: $19 = 3 \cdot 6 + 1 = 3 \cdot 5 + 4 = 3 \cdot 4 + 7$. Portanto 6, 5 e 4 são quocientes, e os restos respectivos são 1, 4 e 7. Mas existe o maior quociente, que no exemplo dado é 6 e que corresponde ao menor resto, 1.

*Dividir* um número natural $a$ por um número natural $b$ tal que $0 < b \leq a$ significa encontrar um quociente $q$ tal que $a = bq$ ou o maior quociente $q$ e o resto $r$ tais que $a = bq + r$. Nesse caso temos $r < b$.

De acordo com o que comentamos acima sobre o significado da divisão estamos considerando duas maneiras de calcular $q$ e $r$.

A primeira é perfazer subtrações sucessivas. Assim, para dividir $a$ por $b$, com $b < a$, calculamos $a - b$, $a - 2b$, $a - 3b$,... Notemos que os valores $a - qb$, para $q = 1, 2, 3,...$ diminuem à medida que $q$ cresce. Assim existe o maior $q$ tal que a subtração $a - qb$ pode ser feita mas $a - (q + 1)b$ não. Se encontrarmos $q$ tal que $a = qb$, a divisão é exata e terminamos. Caso contrário, chamando $r = a - qb$ temos $a = qb + r$, e a divisão terminou. Para dividir $a$ por $b$, com $b = a$, basta tomar $q = 1$, e a divisão é exata.

A segunda maneira de dividir $a$ por $b$, com $b \leq a$, consiste em calcular $1 \cdot b$, $2b$, $3b$,... até atingir o valor $a$ ou ultrapassá-lo. Se o valor $a$ for atingido, significa que encontramos $q$ tal que $a = qb$, e a divisão é exata. Se o valor $a$ não for atingido, seja $qb$ o maior elemento da sequência antes de $a$, de modo que $qb < a < (q + 1)b$. Chamando $r = a - qb$ temos $a = qb + r$, e a divisão terminou.

Observemos que em ambos os casos $r$ é o menor resto possível. De fato, sejam $t$ e $s$ números naturais tais que $a = tb + s$, e suponhamos que $s < r$. Então $a - tb < a - qb$, o que implica $qb < tb$. Disso segue $q < t$, o que contraria a hipótese de ser $q$ o maior número natural tal que $qb < a$. Portanto $r \leq s$.

Destacamos o seguinte resultado, que pode ser muito útil:

*Se $a = bq + r$ com $r < b$, então $q$ é a quantidade de múltiplos de $b$ no conjunto 1, 2, 3, ..., $a$.*

### 3.6.2 Algoritmos para a divisão

Nesta seção o principal objetivo é estudar a gênese do algoritmo usual de divisão, aquele que é ensinado em nossas escolas. Desse modo poderemos compreender por que o algoritmo atingiu seu formato atual. Pensamos que o melhor jeito de fazer esse estudo é considerar alguns exemplos.

Começamos dividindo 30 por 7 através do método de subtrações sucessivas.

$$\begin{array}{l} 30-7=23 \\ 23-7=16 \\ 16-7=\ 9 \\ \ 9-7=\ 2 \end{array} \quad \text{ou} \quad \begin{array}{r} 30 \\ -7 \\ \hline 23 \end{array} \quad \begin{array}{r} 23 \\ -7 \\ \hline 16 \end{array} \quad \begin{array}{r} 16 \\ -7 \\ \hline 9 \end{array} \quad \begin{array}{r} 9 \\ -7 \\ \hline 2 \end{array}$$

Como foram feitas 4 subtrações, então 4 é o quociente. O resto é 2. Assim, $30 = 4 \cdot 7 + 2$.

Podemos facilmente imaginar que o dispositivo acima não seria nada conveniente para dividir números maiores. Dessa forma precisamos encontrar uma forma mais sintética. O dispositivo abaixo, usado para dividir 30 por 7, utiliza o mesmo método de divisões sucessivas, mas adota um formato mais conveniente.

$$\begin{array}{rl|l} 3\ 0 & & 7 \\ \hline -\ 7 & & 1 \\ \hline 2\ 3 & & \\ -\ 7 & & 1 \\ \hline 1\ 6 & & \quad + \\ -\ 7 & & 1 \\ \hline \quad 9 & & \\ -\ 7 & & 1 \\ \hline \quad 2 & & 4 \end{array}$$

Podemos encurtar vendo por exemplo que $3 \times 7 = 21 < 30$, e fazer

$$\begin{array}{rl|l} 3\ 0 & & 7 \\ \hline -\ 2\ 1 & & 3 \\ \hline \quad 9 & & \quad + \\ -\ 7 & & 1 \\ \hline \quad 2 & & 4 \end{array}$$

O melhor mesmo é antecipar que $4 \times 7 = 28 < 30$ fornece o menor resto, e fazer

$$\begin{array}{rl|l} 3\ 0 & & 7 \\ \hline -\ 2\ 8 & & 4 \\ \hline \quad 2 & & \end{array}$$

Podemos sintetizar esse formato eliminando a subtração:

$$\begin{array}{rr|l} 3 & 0 & 7 \\ \cline{3-3} 2 & & 4 \end{array}$$

Acompanhamos mentalmente esse cálculo assim: $4 \times 7 = 28$, para 30, sobram 2. Como $2 < 7$, terminamos.

Para prosseguir, adotaremos a seguinte nomenclatura para a divisão:

em $a = bq + r$ ou em $\begin{array}{l|l} a & b \\ \cline{2-2} \cdot & q \\ \cdot\cdot & \\ r & \end{array}$

temos: $a$ é o dividendo; $b$ é o divisor; $q$ é o quociente, e $r$ é o resto.

Para aperfeiçoar nosso método vejamos um exemplo com um número um pouco maior.

$$\begin{array}{rrr|l} 1 & 2 & 3 & 7 \\ \cline{4-4} -\,7 & 0 & & 1\ 0 \\ \cline{1-1} 5 & 3 & & +\,7 \\ \cline{4-4} -\,4 & 9 & & 1\ 7 \\ \cline{1-1} & 4 & & \end{array}$$

Para dividir 123 por 7 começamos com $10 \times 7 = 70$, e fazemos $123 - 70 = 53$. Observe que não é possível começar com $20 \times 7$ ou um número maior. Podemos economizar escrevendo 1 no quociente no lugar de 10. Depois, ao dividir 53 por 7 colocamos o quociente 7 na frente de 1, obtendo 17. Assim evitamos fazer a soma $10 + 7 = 17$ no quociente. Podemos fazer isso devido a que o dígito 1 do quociente 17 é o maior possível. Ficamos com

$$\begin{array}{rrr|l} 1 & 2 & 3 & 7 \\ \cline{4-4} -\,7 & 0 & & 1\ 7 \\ \cline{1-1} 5 & 3 & & \\ -\,4 & 9 & & \\ \cline{1-1} & 4 & & \end{array} \qquad \text{ou} \qquad \begin{array}{rrr|l} 1 & 2 & 3 & 7 \\ \cline{4-4} 5 & 3 & & 1\ 7 \\ \cline{1-1} & 4 & & \end{array}$$

Vejamos mais um exemplo com o cálculo de 31709 dividido por 8. O método compacto fica

$$\begin{array}{rrrrr|l} 3 & 1 & 7 & 0 & 9 & 8 \\ \cline{6-6} 7 & 7 & & & & 3\ 9\ 6\ 3 \\ \cline{1-1} 5 & 0 & & & & \\ \cline{1-1} 2 & 9 & & & & \\ \cline{1-1} 5 & & & & & \end{array}$$

Para estudar as regras usuais de divisão o estudante pode desenvolver os cálculos com detalhes adicionais, como fazemos a seguir com a divisão anterior. Primeiro consideramos a decomposição $31709 = 31000 + 709$, e calculamos a divisão de 31 por 8. Da tábua de multiplicação sabemos que $8 \cdot 3 < 31 < 8 \cdot 4$. Logo, o melhor divisor é 3, e o resto $31 - 24 = 7$. Obtemos $31 = 8 \cdot 3 + 7$, donde $31000 = 8 \cdot 3000 + 7000$. Em consequência, a decomposição inicial se transforma em

$$31709 = 8 \cdot 3000 + 7000 + 709 = 8 \cdot 3000 + 7709.$$

Procedemos da mesma forma com 7709. Temos $77 = 8 \cdot 9 + 5$, e daí

$$7709 = 7700 + 9 = 8 \cdot 900 + 500 + 9 = 8 \cdot 900 + 509.$$

Agora com 509, calculamos $50 = 8 \cdot 6 + 2$, e então

$$509 = 500 + 9 = 8 \cdot 60 + 20 + 9 = 8 \cdot 60 + 29,$$

e, finalmente,

$$29 = 8 \cdot 3 + 5.$$

Em resumo,

$$\begin{array}{rrrrrl|l}
3 & 1 & 7 & 0 & 9 & & 8 \\
\cline{7-7}
-2 & 4 & 0 & 0 & 0 & & 3\,0\,0\,0 \\
\cline{1-5}
 & 7 & 7 & 0 & 9 & & \quad 9\,0\,0 \\
- & 7 & 2 & 0 & 0 & & \quad +\,6\,0 \\
\cline{1-5}
 & & 5 & 0 & 9 & & \qquad\quad 3 \\
\cline{2-5}
 & - & 4 & 8 & 0 & & 3\,9\,6\,3 \\
\cline{2-5}
 & & & 2 & 9 & & \\
 & & - & 2 & 4 & & \\
\cline{3-5}
 & & & & 5 & &
\end{array}$$

O estudo da gênese do algoritmo usual da divisão coloca em evidência dois dispositivos que lidam com dificuldades específicas do aprendizado da divisão. Um deles é o dispositivo longo, que desmembra as operações de multiplicação e subtração, as quais são realizadas simultaneamente no dispositivo usual, quando se calculam os divisores parciais.

Eis o dispositivo longo:

$$\begin{array}{rrrrrl|l}
3 & 1 & 7 & 0 & 9 & & 8 \\
\cline{7-7}
-2 & 4 & & & & & 3\,9\,6\,3 \\
\cline{1-2}
 & 7 & 7 & & & & \\
- & 7 & 2 & & & & \\
\cline{2-3}
 & & 5 & 0 & & & \\
 & - & 4 & 8 & & & \\
\cline{3-4}
 & & & 2 & 9 & & \\
 & & - & 2 & 4 & & \\
\cline{3-4}
 & & & & 5 & &
\end{array}$$

Comparando o dispositivo longo com o comum, vemos que o primeiro exige menos treinamento e menor uso da memória do que o segundo. Um estudante terá menos dificuldade em aprender o algoritmo da divisão se iniciar com o método longo, e, depois de o ter dominado, estudar o método comum.

O outro dispositivo lida com o processo de tentativa e erro no cálculo dos quocientes parciais. No cálculo a seguir, o quociente de 77 por 8 foi subestimado, o que ficou evidente pelo fato de ser o resto 13 maior do que 8. Para corrigir, basta somar 1 ao quociente parcial e subtrair 8 de 13. Após isso, o cálculo continua normalmente. Esse dispositivo é especialmente adequado quando o divisor tem dois ou mais dígitos. Seu uso facilita para o estudante a correção de erro para menos na estimativa dos quocientes parciais e pode traduzir uma oportunidade de melhor compreensão do mecanismo do algoritmo usual.

$$\begin{array}{rrrrrl|l}
 & 3 & 1 & 7 & 0 & 9 & 8 \\
\cline{7-7}
- & 2 & 4 & & & & 3\ 8 \\
\cline{1-3}
 & & 7 & 7 & & & +\ 1 \\
\cline{2-4}
 & - & 6 & 4 & & & 3\ 9\ 6\ 3 \\
\cline{2-4}
 & & 1 & 3 & & & \\
 & & - & 8 & & & \\
\cline{3-4}
 & & & 5 & 0 & & \\
 & & - & 4 & 8 & & \\
\cline{3-5}
 & & & & 2 & 9 & \\
 & & & - & 2 & 4 & \\
\cline{4-5}
 & & & & & 5 &
\end{array}$$

O método usual de divisão se aplica em qualquer sistema numérico posicional. Vejamos um exemplo na base quinária (base cinco).

$$\begin{array}{rrrl|l}
 & 4 & 2 & 3 & 1\ 2 \\
\cline{5-5}
 & & & & 3\ 1 \quad _{cinco} \\
- & 4 & 1 & & \\
\cline{2-3}
 & & 1 & 3 & \\
 & - & 1 & 2 & \\
\cline{3-4}
 & & & 1 &
\end{array}$$

Vimos, no Capítulo 2, diversos exemplos de mudanças de base em sistemas numéricos posicionais. Ali, todas as mudanças eram feitas usando-se a base dez como intermediária, mas observamos que existem formas diretas de transposição. Com os conhecimentos adquiridos neste capítulo, podemos efetuar mudanças de base diretamente, sem passar pela base dez.

Como exemplo calculamos a seguir a representação de $(325)_{seis}$ na base oito. Podemos proceder de duas formas. A primeira consiste em expandir $(325)_{seis}$ na base seis e fazer os cálculos na base oito:

$$\begin{aligned}
(325)_{seis} &= 3 \cdot 6^2 + 2 \cdot 6 + 5 \\
&= 3 \cdot (44)_{oito} + (14)_{oito} + 5 \\
&= (154)_{oito} + (14)_{oito} + 5 \\
&= (175)_{oito} \, .
\end{aligned}$$

A segunda forma consiste em fazer divisões sucessivas de $(325)_{seis}$ por $(12)_{seis}$ na base seis. Observe o estudante que $(12)_{seis}$ é a representação de oito na base seis. Temos

$$\begin{array}{rrr|l}
 & 3 & 2 & 5 \\
\cline{4-4}
 & & & 1\ 2 \quad _{seis} \\
- & 2 & 4 & \\
\cline{2-3}
 & 0 & 4 & 5 \\
 & - & 4 & 0 \\
\cline{3-4}
 & & & 5
\end{array}
\qquad
\begin{array}{rr|l}
 & 2 & 3 \\
\cline{3-3}
 & & 1\ 2 \quad _{seis} \\
- & 1 & 2 \\
\cline{2-2}
 & 1 & 1
\end{array}
\qquad
\begin{array}{r|l}
 & 1 \\
\cline{2-2}
 & 1\ 2 \quad _{seis} \\
1 & 0
\end{array}$$

Os restos obtidos são $1_{seis}$, $11_{seis}$ e $5_{seis}$. Na base oito esses restos são $1_{oito}$, $7_{oito}$ e $5_{oito}$, e eles são os dígitos procurados, ou seja,

$$(325)_{seis} = (175)_{oito} \, .$$

A mais antiga forma de divisão conhecida pela História da Matemática é a que era utilizada pelos egípcios da Antiguidade. Vamos dar um exemplo do método com o cálculo de 250 dividido por 7.

Dispomos os cálculos em duas colunas:

| | | |
|---|---|---|
| $\star$ | 1 | 7 |
| $\star$ | 2 | 14 |
| | 4 | 28 |
| | 8 | 56 |
| | 16 | 112 |
| $\star$ | 32 | 224 |
| | | 245 |

Na segunda coluna começamos com o divisor 7 e o duplicamos sucessivamente até obter um número menor ou igual a 250 e maior do que a metade de 250 (portanto, o número seguinte seria maior do que 250). Na primeira coluna, colocamos as potências de 2, começando com $2^0 = 1$.

O próximo passo do método consiste em procurar, entre os números da segunda coluna, aqueles cuja soma seja menor ou igual a 250, o mais próxima possível. Vemos que $7+14+224 = 245$, e essa é a soma mais próxima de 250 que podemos obter com os números da segunda coluna. Assinalamos com $\star$ as linhas que contêm os números escolhidos na segunda coluna.

Finalmente, adicionamos os números da primeira coluna que estão nas linhas assinaladas por $\star$ : $1 + 2 + 32 = 35$. Esse é o quociente. O resto é $250 - 245 = 5$.

### 3.6.3 Problemas

**Problema 3.6.3.1.** Um dia um professor repartiu um pacote de biscoitos entre 12 estudantes, cabendo 5 para cada, e sobraram 6 biscoitos. Em outro dia, um pacote de biscoitos igual ao anterior foi repartido entre 5 estudantes, e sobraram menos do que 5 biscoitos. Quantos biscoitos couberam a cada estudante na segunda distribuição?

**Problema 3.6.3.2.** Vejamos a divisão de 13 732 por 17 segundo as regras usuais. Como $1 < 17$, pegamos 13; como $13 < 17$, pegamos 137, que dividido por 17 tem 8 como o maior divisor possível. Sobra 1, que colocamos abaixo do dígito 7 do dividendo. Abaixamos o dígito 3 do dividendo. Como $13 < 17$, colocamos zero no divisor, e em seguida abaixamos o dígito 2 do dividendo. Ficamos com 132, que dividido por 17 dá 7, e o resto é 13. O cálculo final tem a seguinte forma:

| | |
|---|---|
| 1 3 7 3 2 | 1 7 |
| 1 3 2 | 8 0 7 |
| 1 3 | |

Explique por que devemos colocar um zero no divisor.

**Problema 3.6.3.3.** Um estudante calculou $701 \div 23$ usando o algoritmo longo. Achou 3 como quociente e 11 como resto. Usando cálculo mental, o professor logo percebeu que estava errado. Como ele fez isso? Qual foi a provável causa do erro do estudante?

**Problema 3.6.3.4.** Faça as seguintes mudanças de base, sem utilizar a base dez como intermediária. Use ambas as formas explicadas no texto. **a)** $(212)_{três}$ para a base cinco; **b)** $(408)_{nove}$ para a base sete.

**Problema 3.6.3.5.** Estude a seguinte a seguinte disposição do algoritmo usual de divisão utilizado em alguns países:

$$\begin{array}{rrl} & 3\,9\,6\,3 & \longleftarrow \text{quociente} \\ \text{divisor} \longleftarrow\ 8 \ \big| & 3\,1\,7\,0\,9 & \longleftarrow \text{dividendo} \\ & \underline{2\,4} & \\ & \ \ 7\,7 & \\ & \ \ \underline{7\,2} & \\ & \ \ \ \ 5\,0 & \\ & \ \ \ \ \underline{4\,8} & \\ & \ \ \ \ \ \ 2\,9 & \\ & \ \ \ \ \ \ \underline{2\,4} & \\ & \ \ \ \ \ \ \ \ 5 & \longleftarrow \text{resto} \end{array}$$

**Problema 3.6.3.6.** O sinal $\div$ pode ser utilizado para indicar a operação de divisão. Efetue as seguintes divisões nas bases solicitadas usando o algoritmo usual:

$$(34203)_{cinco} \div (3)_{cinco}\ ;$$

$$(402103)_{cinco} \div (23)_{cinco}\ ;$$

$$(1100110)_{dois} \div (11)_{dois}\ ;$$

$$(53024)_{sete} \div (61)_{sete}\ ;$$

$$(9AB08)_{doze} \div (25)_{doze}\ .$$

**Problema 3.6.3.7.** Vimos em (3.16) que quando a divisão dos números naturais $a$ por $b$ é exata, existe $q$ tal que $a = bq$. Nesse caso, a notação fracionária de $q$ é $q = \frac{a}{b}$. Todo número natural $a$ é uma fração, pois $a = a \cdot 1$ implica a notação $a = \frac{a}{1}$. Demonstre: (i) dados $q = \frac{a}{b}$ e $p = \frac{c}{d}$, temos $\frac{a}{b} \pm \frac{c}{d} = \frac{ad \pm bc}{bd}$ e $\frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}$; (ii) Para todo número inteiro $m$ temos $m + \frac{a}{b} = \frac{mb+a}{b}$ e $m \times \frac{a}{b} = \frac{ma}{b}$. (iii) $\frac{ab}{ac} = \frac{b}{c}$; (iv) $\frac{a}{b} \Big/ \frac{c}{d} = \frac{ad}{bc}$.

**Problema 3.6.3.8.** Sejam $a$ e $b$ números naturais. Suponha que ao "dividir" $a$ por $b$ de várias formas se encontrem números naturais $q$, $t$, $r$ e $s$ tais que $a = bq + r$ e $a = bt + s$. Por exemplo, se $a = 23$ e $b = 3$ podemos ter $a = 7b + 2$ e $a = 6b + 5$. **a)** Identifique alguma regularidade sobre $r$ e $s$ nessas situações. **b)** Se $r, s < b$, o que mais se pode afirmar?

## 3.7 A potenciação

Já estivemos usando notações como $a^2$ e $10^n$, contando com o conhecimento prévio do estudante. Vejamos agora alguns detalhes sobre a denominada *operação de potenciação*. A potenciação, como o próprio nome diz, potencializa a multiplicação. Ela é muito útil para sintetizar e facilitar cálculos algébricos.

*Potenciação* é o nome que se dá à multiplicação de valores repetidos. Quaisquer que sejam os números naturais $a$ e $n$, anotamos

$$a \cdot a \cdot a \cdots a = a^n \qquad (a \text{ multiplicado por ele mesmo } n \text{ vezes}).$$

Aqui se entende que $a^1 = a$. Na notação $a^n$, dizemos que $a$ é a *base* e $n$ é o *expoente*. Dizemos também que $a^n$ é a *potência n-ésima* de $a$.

As seguintes propriedades são fáceis de constatar:

*Propriedade 1: potências de mesma base:* quaisquer que sejam os números naturais $a$, $m$ e $n$, temos

$$a^{m+n} = a^m a^n.$$

Para ver que essa fórmula é válida, basta juntar as parcelas de $a^m a^n$:

$$a^m \cdot a^n = \underbrace{a\,a\cdots a}_{m} \cdot \underbrace{a\,a\cdots a}_{n} = \underbrace{a\,a\cdots a}_{m+n} = a^{m+n}.$$

*Propriedade 2: potência de potência:* quaisquer que sejam os números naturais $a$, $m$ e $n$, temos

$$(a^m)^n = a^{mn}.$$

Para ver que essa fórmula é válida, basta reorganizar os produtos de $a$:

$$(a^m)^n = \overbrace{a^m\, a^m \cdots a^m}^{n} = \overbrace{\underbrace{a\,a\cdots a}_{m} \cdot \underbrace{a\,a\cdots a}_{m} \cdots \underbrace{a\,a\cdots a}_{m}}^{n} = \underbrace{a\,a\cdots a}_{mn} = a^{mn}.$$

*Propriedade 3: potências de mesmo expoente:* quaisquer que sejam os números naturais $a$, $b$ e $m$, temos

$$a^m b^m = (ab)^m.$$

Para ver que essa fórmula é válida, basta reorganizar os produtos de $a$ e $b$ usando a propriedade comutativa da multiplicação:

$$a^m b^m = \underbrace{a\,a\cdots a}_{m} \cdot \underbrace{b\,b\cdots b}_{m} = \underbrace{ab\,ab\cdots ab}_{m} = (ab)^m.$$

Observamos que a notação $a^{m^n}$ não é determinada. Ela pode significar $(a^m)^n$, em que primeiro se calcula $a^m$ e ao resultado se aplica o expoente $n$, ou pode significar $a^{(m^n)}$, em que primeiro se calcula $m^n$, e o resultado é a potência $m^n$-ésima de $a$. O mesmo vale para expressões como

$$a^{m^{n^p}} \qquad \text{e} \qquad a^{m^{m^{m^m}}}$$

**Convenção.** Neste texto fazemos a seguinte convenção:

$$a^{m^n} = a^{(m^n)}.$$

Em geral, em tais expressões, as potências são calculadas de cima para baixo, mas isso não é obrigatório. É preciso que o autor deixe isso claro no texto.

### 3.7.1 Problemas

**Problema 3.7.1.1.** Mostre que os valores de $2^{2^3}$ e de $2^{2^{2^{2^2}}}$ dependem da ordem com que as potências são calculadas.

**Problema 3.7.1.2.** Sejam $a$, $m$ e $n$ números naturais quaisquer. Explique por que $(a^m)^n = (a^n)^m$.

**Problema 3.7.1.3.** Escreva de forma sintética a expressão $7^n + 7^n + 7^n + 7^n + 7^n + 7^n + 7^n$.

**Problema 3.7.1.4.** Qual é a soma dos dígitos de $2^{25}5^{20}$ ?

**Problema 3.7.1.5.** Sejam $a$, $b$ e $m$ números naturais quaisquer. Demonstre que: (i) $a = b \Rightarrow a^m = b^m$; (ii) $a < b \Rightarrow a^m < b^m$; (iii) $a^m = b^m \Rightarrow a = b$; (iv) $a^m < b^m \Rightarrow a < b$.

Em resumo, $a = b$ se, e somente se, $a^m = b^m$, e $a < b$ se, e somente se, $a^m < b^m$.

**Problema 3.7.1.6.** (a) Descubra qual desses números é maior: $2^{23}$ e $3^{17}$. (b) É possível encontrar $m$ e $n$ tais que $2^m = 3^n$?

**Problema 3.7.1.7.** Sejam $a > 1$, $m$ e $n$ números naturais quaisquer. (i) Demonstre que $a^n < a^m$ se, e somente se, $n < m$. (ii) Demonstre que $a^n = a^m$ se, e somente se, $n = m$.

**Problema 3.7.1.8.** Sejam $a$, $m$ e $n$ números naturais tais que $m > n$. Qual é o quociente e o resto da divisão de $a^m$ por $a^n$ ?

**Problema 3.7.1.9.** Sejam $a$, $m$ e $n$ números naturais quaisquer. (i) Demonstre que se $b \cdot a^n < a^m$, então $n < m$ e $b < a^{m-n}$. (ii) Demonstre que se $n < m$ e $a^m < b \cdot a^n$, então $a^{m-n} < b$.

**Problema 3.7.1.10.** Calcule os números naturais $m$ para os quais vale a expressão $50^3 < 5^m < 50^4$.

## 3.8 Verificação de cálculos aritméticos

Nos dias atuais o trabalho de realizar cálculos aritméticos está muito facilitado com o uso das calculadoras eletrônicas. Por isso existe hoje um desinteresse a respeito dos métodos de verificação do acerto de cálculos aritméticos. Mas, para completar a formação do estudante em Aritmética, não poderíamos terminar esse capítulo sem comentar brevemente alguns desses métodos.

A verificação mais imediata de um cálculo aritmético consiste em repetir as contas. Pode ser útil modificar a situação inicial, por exemplo, na adição e na multiplicação podemos repetir o cálculo trocando a ordem das parcelas. Podemos também verificar um cálculo aritmético usando a chamada *prova real*, que consiste em verificar a operação realizando a operação inversa.

Tira-se a prova real de uma adição por meio da subtração. Por exemplo,

$$\begin{array}{r} 37589 \\ +\,29805 \\ \hline 67394 \end{array} \qquad \text{prova:} \qquad \begin{array}{r} 67394 \\ -\,29805 \\ \hline 37589 \end{array}$$

Tira-se a prova real de uma subtração somando-se o subtraendo com o resto. O resultado deve ser o minuendo. Pode-se também subtrair o resto do minuendo. O resultado deve ser o oposto do subtraendo.

A prova real da multiplicação consiste em dividir o produto por um dos fatores. O quociente deve ser o outro fator, e o resto, zero. Por outro lado, a prova real da divisão consiste em multiplicar o divisor pelo quociente, e ao produto assim obtido soma-se o resto da divisão. O resultado deve ser o dividendo.

Se a aplicação de uma prova dá resultado positivo conclui-se que o cálculo original está provavelmente correto. Pode-se cometer na prova um erro que compense algum engano feito no primeiro cálculo, mas é pouco provável que ocorra essa coincidência.

Vejamos a chamada *prova do nove*. Começamos explicando a antiga expressão "tirar os noves fora". Dado um número natural $a > 9$, formamos o número natural $s(a)$ obtido com a soma

dos dígitos decimais de $a$. Por exemplo, $s(160) = 1+6+0 = 7$, e $s(8\,714) = 8+7+1+4 = 20$. Se $a = 9$, pomos $s(9) = 0$.

Observamos que para todo número natural $a$, $s(a)$ é um resto da divisão de $a$ por 9. Por exemplo, $367 = 3 \cdot 100 + 6 \cdot 10 + 7 = 3(99+1) + 6(9+1) + 7 = 3 \cdot 99 + 3 + 6 \cdot 9 + 6 + 7 = 9q + (3+6+7) = 9q + s(a)$, para um certo número natural $q$. Portanto, $s(a)$ é um resto da divisão de $a$ por 9. O estudante é convidado a fazer uma demonstração geral desse fato no Problema 6.6.9.

"Tirar os noves fora" de um número $a$ significa aplicar sucessivamente a operação $s(a)$ até que se obtenha um número $< 9$, que é o menor resto da divisão de $a$ por 9. Isso sempre é possível, pois se $a \geq 9$ então $s(a) < a$.

Na prática, podemos descartar o valor 9 à medida que somamos os dígitos do número dado. Por exemplo, se $a = 86946$, somamos $8 + 6 = 14$, e já fazemos $1 + 4 = 5$, e ficamos com 5. Descartamos o dígito seguinte, que é 9, e fazemos $5 + 4 = 9$, que é descartado. Fica 6, que é o menor resto da divisão de $a = 86946$ por 9. Esse procedimento inspirou o nome "tirar os noves fora".

Observamos agora que se $a$, $b$ e $c$ são números naturais tais que $a + b = c$, então $r(r(a) + r(b)) = r(c)$, de acordo com o Problema 6.6.10. Essa é a prova do nove para a adição. Vejamos um exemplo.

$$\begin{array}{rcr} 94795 & \longrightarrow & 7 \\ +\,87367 & \longrightarrow & +\,4 \\ \hline 182162 & & 11 \\ \downarrow & & \downarrow \\ 2 & & 2 \end{array}$$

Observe que 94795 noves fora é 7, e 87367 noves fora é 4. Temos $7 + 4 = 11$, e 11 noves fora é 2. Como 182 162 noves fora é também 2, vemos que o cálculo passa pela prova do nove.

Se um cálculo de adição não passa pela prova do nove, então ele está errado, conforme já observamos. Mas a recíproca dessa afirmação não é verdadeira. Isto é, se um cálculo de adição passa pela prova do nove, o cálculo não está necessariamente correto. Por exemplo,

(incorreto)
$$\begin{array}{rcr} 94795 & \longrightarrow & 7 \\ +\,87367 & \longrightarrow & +\,4 \\ \hline 183152 & & 11 \\ \downarrow & & \downarrow \\ 2 & & 2 \end{array}$$

Vemos nesse exemplo que a prova do nove não detectou o erro. Se a prova do nove não revela erro em um cálculo de adição, então a soma verdadeira e a soma incorreta diferem de um múltiplo de 9. A probabilidade disso ocorrer é relativamente baixa, e por isso se diz que se o cálculo passa pela prova, então ele está provavelmente correto.

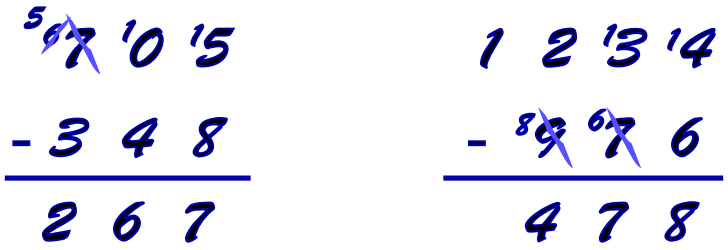
De forma análoga podemos aplicar a prova do nove para a subtração, a multiplicação e a divisão. A prova dos nove também não é conclusiva para essas operações.

## 3.9 Problemas adicionais

**Problema 3.9.1.** Argumente a validade da seguinte sentença: se $a = b$ e $c = d$, então $a - c = b - d$ (desde que as subtrações sejam possíveis).

**Problema 3.9.2.** Em uma escola foi pedido a um estudante calcular $12 + 15$. Ele fez alguns cálculos com os dedos e respondeu: 9. Que hipótese você pode supor sobre esse erro?

**Problema 3.9.3.** Estudantes fizeram os cálculos descritos abaixo. Descubra os passos que seguiram e o que os levou a cometer esses erros.



**Problema 3.9.4.** Elabore regras sintéticas para se calcular a soma de quatro número naturais consecutivos. E quanto a seis números consecutivos?

**Problema 3.9.5.** Explique por que nunca se usou uma "prova do cinco", em vez da prova do nove, na verificação de cálculos aritméticos.

**Problema 3.9.6.** Encontre um método de verificação de cálculos aritméticos equivalente à prova do nove em sistemas de numeração em outras bases. Dê alguns exemplos na base quatro. Como se aplica o método na base dois?

**Problema 3.9.7.** Demonstre que se um número terminado em 5 (no sistema decimal) é quadrado de um número natural, então o dígito das dezenas é 2.

**Problema 3.9.8.** Uma *grosa* é igual a doze dúzias. Usando aritmética duodecimal, resolva os seguintes problemas. **a)** Um comerciante tinha dez grosas de ovos. Vendeu 5 grosas, 7 dúzias e 8 unidades. Quanto restou? **b)** Três sócios devem repartir uma produção de dezessete grosas, oito dúzias e onze unidades de ovos. Quanto caberá a cada um?

**Problema 3.9.9.** Em um antigo livro didático [118] o autor exemplifica a subtração $8003004 - 2758436$ da seguinte forma:

$$\begin{array}{rccccccc} & & & & 12 & & & \\ & 7 & 9 & 9 & 2 & 9 & 9 & 14 \\ & 8 & 0 & 0 & 3 & 0 & 0 & 4 \\ - & 2 & 7 & 5 & 8 & 4 & 3 & 6 \\ \hline & 5 & 2 & 4 & 4 & 5 & 6 & 8 \end{array}$$

Desvende o que foi feito.

**Problema 3.9.10.** Um estudante, ao efetuar $(5114)_{seis} - (3532)_{seis}$ na base seis, procedeu da seguinte forma. Primeiro fez a conta na base dez, como se os números estivessem na base dez:

$$\begin{array}{r} 5\,1\,1\,4 \\ -3\,5\,3\,2 \\ \hline 1\,5\,8\,2 \end{array}$$

Depois, substituiu os dígitos 5 e 8 do número assim obtido pelas diferenças $5 - 4 = 1$ e $8 - 4 = 4$, obtendo o número $(1142)_{seis}$ , que afirmou ser a resposta correta. Confira o resultado e explique. Investigue se o método funciona em outras bases.

**Problema 3.9.11.** Um indivíduo, visitando um país exótico, soube que ali se usava um sistema numérico posicional com algarismos 0, 1, 2, ..., e que o nome da unidade monetária era rupi. Em uma loja, deu ao comerciante uma nota de 400 rupis para pagar 135 rupis. O comerciante pediu 5 rupis para facilitar o troco, que foi de 250 rupis. Qual era a base do sistema numérico?

**Problema 3.9.12.** Um país de cultura antiga tem três tipos de moeda: a de menor valor, pini, a de valor intermediário, marc, e a de maior valor, drac. Um turista, para pagar uma conta de 7 marcs e 8 pinis em um restaurante, deu 1 drac, e recebeu de troco 1 marc e 4 pinis. Observando depois que 9 pinis perfazia quase 10% da conta, deu-os ao garçon.

Calcule quantos pinis vale 1 marc, e quantos marcs vale 1 drac.

**Problema 3.9.13.** Calculando algumas potências quínticas de números naturais observamos que o número e sua potência sempre têm a mesma unidade. Justifique por que isso ocorre para qualquer número natural.

**Problema 3.9.14.** Confira os seguintes cálculos: $9 \times 9 = 81$ na base dez, $4 \times 4 = 31$ na base cinco, $8 \times 8 = 71$ na base nove. Que regularidade pode ser observada? Dê uma fórmula que generalize esses produtos em uma base qualquer $\beta$, e justifique.

**Problema 3.9.15.** Observe que na base decimal $9 + 9 = 18$ é o reverso de $9 \times 9 = 81$. Mostre que uma situação análoga ocorre em um sistema posicional de base $\beta$ qualquer.

**Problema 3.9.16.** Note que na tábua de multiplicação do 9 na base dez a soma dos dígitos de qualquer produto é sempre 9 (exceto para $9 \times 0$). Generalize para uma base qualquer.

**Problema 3.9.17.** A *regra turca* para calcular o produto de dois algarismos situados entre 7 e 9 pode ser exemplificada com o cálculo de $7 \times 8$. Mantemos uma das mãos com dois dedos levantados, os quais correspondem a $7-5 = 2$. Na outra mão, mantemos três dedos levantados, que correspondem a $8 - 5 = 3$. O produto $7 \times 8 = (a_1a_2)_{10}$ é assim calculado: o dígito das dezenas $a_1$ é o total dos dedos levantados, no caso $a_1 = 2 + 3 = 5$; o dígito das unidades $a_0$ é o produto dos números dos dedos que não estão levantados em cada mão. No caso, $a_0 = 3 \times 2 = 6$. Portanto, $7 \times 8 = 56$. Dê uma demonstração algébrica para a regra turca.

**Problema 3.9.18.** Encontre o dígito $d$ que está faltando para completar a seguinte multiplicação:

$$9\,966\,334 \times 9\,966\,332 = 99\,327\,d93\,466\,888.$$

**Problema 3.9.19.** O algoritmo usual de adição pode ser descrito algebricamente. Estude a seguinte versão. Utilize-a para implementar $67493 + 4568$.

Notemos primeiro que dois números naturais $a$ e $b$ podem ser representados no sistema decimal com a mesma quantidade de dígitos, bastando para isso acrescentar o algarismo zero à esquerda de um deles, se necessário.

Sejam então $a = (a_n a_{n-1} \dots a_1 a_0)$ e $b = (b_n b_{n-1} \dots b_1 b_0)$. Para calcular $a + b$ devemos executar os seguintes passos, com $i = 1, 2, \dots, n$:

(*passo 0*) calcular os números naturais $q_0$ e $c_0$ tais que $a_0 + b_0 = q_0 \cdot 10 + c_0$, com $q_0 = 0$ ou 1 e $0 \leq c_0 \leq 9$;

(*passo i*) calcular os números naturais $q_i$ e $c_i$ tais que $a_i + b_i + q_{i-1} = q_i \cdot 10 + c_i$, com $q_i = 0$ ou 1 e $0 \leq c_i \leq 9$.

A soma é $a + b = (q_n c_n c_{n-1} \dots c_1 c_0)$.

**Problema 3.9.20.** Estude a seguinte descrição algébrica do algoritmo usual da subtração. Aplique o algoritmo para calcular $3534 - 2627$.

Sejam $a = (a_n \dots a_1 a_0)$ e $b = (b_n \dots b_1 b_0)$ números naturais tais que $a > b$. Para encontrar a diferença $a - b$, procedemos as seguintes etapas, com $1 \leq i \leq n$:

(*passo 0*) calcular os números inteiros $q_0$ e $c_0$ tais que $a_0 - b_0 = q_0 10 + c_0$, com $0 \leq c_0 \leq 9$. Temos $q_0 = 0$ se $a_0 \geq b_0$, e $q_0 = -1$ se $a_0 < b_0$ (nesse caso, $q_0$ é o "empréstimo").

(*passo i*) calcular os números inteiros $q_i$ e $c_i$ tais que $a_i - b_i + q_{i-1} = q_i 10 + c_i$, com $0 \leq c_i \leq 9$, e $q_i = 0$ ou $-1$.

Como $a > b$, vem que $q_n = 0$. A diferença procurada é $a - b = (c_n \dots c_1 c_0)$.

**Problema 3.9.21.** Explique o seguinte procedimento de adivinhação. Comece com dois números naturais não nulos menores do que dez (não necessariamente diferentes). Multiplique o primeiro por 2 e adicione 5. Multiplique o resultado por 5, e some 10. Adicione o segundo número, e subtraia 35. Resulta um número com dois dígitos; o dígito das dezenas é o primeiro dos dois números iniciais, e o dígito das unidades, o segundo.

**Problema 3.9.22.** Verifique os seguintes procedimentos de adivinhação de números. **a)** Escolha um número de dois algarismos $(ab)_{dez}$. Multiplique-o por 15, e depois por 7. Subtraia o quádruplo do número. Obtém-se $(abab)_{dez}$. **b)** Escolha um número de dois algarismos $(ab)_{dez}$. Multiplique-o por 13, e depois por 8. Subtraia o triplo do número. Obtém-se $(abab)_{dez}$.

**Problema 3.9.23.** Verifique o seguinte procedimento de adivinhação. Dado um número (natural), multiplique-o por 5, e adicione 6. Em seguida, multiplique o resultado por 4 e adicione 9. Finalmente, multiplique por 5. Elimine do final da representação do resultado o agrupamento 65. Do número resultante, subtraia 1. Esse é o número inicial.

**Problema 3.9.24.** Escolha três algarismos, não necessariamente diferentes, sendo que pelo menos um deles deve ser não nulo. Tome o primeiro algarismo (que não seja nulo), multiplique-o por 5, e adicione 3. Dobre o resultado e adicione o segundo algarismo. Multiplique por 10 e adicione o terceiro algarismo. Subtraia 60. O resultado é um número com três dígitos. O dígito das centenas é o primeiro algarismo escolhido. O dígito das dezenas é o segundo algarismo escolhido, e o das unidades, o terceiro. Por que funciona?

**Problema 3.9.25.** Pense em um número natural maior do que ou igual a 20. Some seus dígitos, e subtraia essa soma do número inicial. Cancele um dígito qualquer do resultado. Some os dígitos do número resultante, obtendo-se um número $a$. Pode-se tentar "adivinhar" o dígito cancelado a partir do conhecimento de $a$. Temos dois casos: *1º caso*: $a$ não é divisível por 9. Então o dígito cancelado é o número que é preciso somar a $a$ para que ele se torne divisível por 9. *2º caso*: $a$ é divisível por 9. Então o dígito cancelado é zero ou 9. Explique.

**Problema 3.9.26.** Confira a seguinte brincadeira com dados. Jogue um dado cúbico três vezes, e anote os números obtidos. Para melhor explicar, suponhamos que estes números tenham sido 1, 2 e 4. Considere em sequência os números das faces opostas, respectivamente, 6, 5 e 3. Forme o número 124653. Divida-o por $37 \times 3$, do quociente subtraia 7, e divida a diferença por 9. O número obtido será 124, que recupera os dígitos iniciais sorteados. Demonstre que isso sempre ocorre, quaisquer que sejam os dígitos iniciais sorteados. Como ficaria essa brincadeira com dados octaedrais?

**Problema 3.9.27.** Demonstre a seguinte mágica com o número 1089. Tome um número com três dígitos, de modo que a diferença entre os dígitos dos extremos seja $\geq 2$. Tome o reverso desse número e faça a diferença (do maior subtrai-se o menor). Tome o reverso da diferença. A soma do terceiro número com o quarto é 1089.

**Problema 3.9.28.** Tome um número de três dígitos, por exemplo 716. Considere o número 716 716. Divida-o por 7, depois por 11, e finalmente por 13. Obtém-se o número inicial 716. Verifique e explique por que isso funciona para qualquer número de três dígitos.

**Problema 3.9.29.** Considere todos os números constituídos pelas permutações dos dígitos 1, 2, 3, 4, 5, 6, 7, 8 e 9. Alguns desses números são 123456789, 213456789, 231456789. **a)** Calcule a quantidade dos números assim obtidos. **b)** Calcule a soma de todos esses números.

**Problema 3.9.30.** Descreva os números naturais $a$ e $b$ tais que $ab > a + b$.

Uma *balança de dois pratos sem escala* é um dispositivo mecânico que permite comparar o peso de dois objetos, isto é, colocando-se um objeto em um prato e outro no segundo prato, o dispositivo indica se os objetos têm o mesmo peso ou qual dos dois é o mais pesado.

**Problema 3.9.31.** São dadas $n$ moedas idênticas na aparência. Todas têm o mesmo peso, exceto uma, que é um pouco mais pesada do que as outras. Elabore procedimentos que permitam encontrar a moeda mais pesada usando uma balança de dois pratos sem escala. Encontre fórmulas para o número de pesagens, ou cotas superiores para esse número.

Um *sistema de pesos para uma balança de dois pratos sem escala* consiste de um conjunto de peças $\mathbf{p}_0$, $\mathbf{p}_1$, $\mathbf{p}_2$, ..., $\mathbf{p}_n$ satisfazendo às condições: **a)** cada peça $\mathbf{p}_i$ pesa $p_i \in \mathbb{N}$ unidades de massa, e $1 = p_1 \leq p_2 \leq \ldots \leq p_n$; **b)** todo número natural de 1 a $p_0 + p_1 + \ldots + p_n$ inclusive tem uma representação balanceada $p_j + \sigma_{j-1}p_{j-1} + \ldots + \sigma_0 p_0$, sendo $\sigma_i = -1$, 0 ou 1 para todo $0 \leq i \leq j$ para algum $j \leq n$.

Nessas condições se diz também que os números $p_0$, $p_1$, $p_2$, ..., $p_n$ constituem um sistema de pesos para uma balança de dois pratos sem escala. A condição **b)** significa que todo objeto com peso inteiro $\leq p_0 + p_1 + \ldots + p_n$ pode ter seu peso avaliado com as peças. A peça $\mathbf{p}_i$ será colocada no mesmo prato em que está o objeto se $\sigma_i = -1$, e no prato oposto se $\sigma_i = 1$. A peça não será utilizada na pesagem se $\sigma_i = 0$ ($p_i$ não comparece na representação).

**Problema 3.9.32.** Demonstre que os seguintes conjuntos de números naturais constituem um sistema de pesos para uma balança de dois pratos sem escala: **a)** 1, 2, 4, 8 e 16; **b)** 1, 3, 9 e 27; **c)** 1, 1, 2, 5, 10, 10, 20, 50, 100.

## 3.10 Sugestões de atividades

**Atividade 3.10.1.** Imagine uma forma de explicar para crianças que a soma de vários números naturais pode ser calculada tomando-se as parcelas em qualquer ordem. E quanto à multiplicação?

**Atividade 3.10.2.** Consultando livros escolares usados para crianças, veja como os autores trabalham os conceitos das operações aritméticas.

**Atividade 3.10.3.** Pesquise em bibliografia especializada sobre a conveniência ou não de se adotar nas escolas o ensino da aritmética através de ábacos, e só depois disso utilizar a linguagem escrita. Quanto ao ensino da aritmética para adultos, uma possibilidade é consultar [30].

**Atividade 3.10.4.** Pesquise em bibliografia especializada opiniões sobre o ensino de técnicas mentais para as operações aritméticas, e também sobre métodos aproximados.

**Atividade 3.10.5.** Um estudante, pretendendo evitar o uso do "vai um", inventou o seguinte dispositivo para somar dois números com dois dígitos:

$$\begin{array}{r} 27 \\ +19 \\ \hline \end{array} \longrightarrow \begin{array}{r} 20+\ 7 \\ +10+\ 9 \\ \hline 30+16 \end{array} \longrightarrow \begin{array}{r} 30 \\ +16 \\ \hline 46 \end{array}$$

**a)** Esse método sempre evita o transporte da dezena? **b)** O estudante compreendeu a estrutura da representação posicional? **c)** Investigue se é viável utilizar o método do estudante nas

escolas, ensinando-o antes do método usual. Pesquise em bibliografia especializada ou consulte professores da escola básica. **d)** Se um professor resolver ensinar primeiro o método do estudante e depois o método usual, como ele irá mostrar para os estudantes a necessidade de estudar o método usual?

**Atividade 3.10.6.** Foi solicitado de um estudante calcular $63787 \div 3$. Ele fez o seguinte:

$$\begin{array}{rl|l} 6\,3\,7\,8\,7 & & 3 \\ \hline 0\,0\,1\,2\,1 & & 2\;1\;2\;2\;2 \\ \quad 0\,1 & & \quad +\,4 \\ \hline & & 2\;1\;2\;6\;2 \end{array}$$

A conclusão do estudante foi: o quociente é 21262 e o resto é 1.

**a)** Verifique se o resultado está correto. **b)** Verifique se o método utilizado pelo estudante está correto, levando em conta a estrutura do sistema de representação decimal e o algoritmo da divisão. **c)** Verifique se o método funciona bem em outras situações, por exemplo: $708039 \div 8$; $31729 \div 6$; $310012 \div 2$. **d)** O estudante mostrou que compreendeu a estrutura do sistema de representação decimal? O estudante mostrou que compreendeu o mecanismo do algoritmo usual de divisão? O método usado pelo estudante deve ser ensinado para os colegas de classe? Esse método deveria substituir o algoritmo usual? O professor deve proibir o estudante de usar esse método em suas avaliações formais?

**Atividade 3.10.7.** Em uma atividade (adaptada) para crianças da escola básica, um livro texto pede decomposições de 8 como soma de três números. As crianças podem trabalhar com barras na forma concreta ou representadas por desenhos, ou usando uma balança de equilíbrio, ou outras formas. A Figura 3.5 ilustra uma possibilidade. Essa atividade pode anteceder o aprendizado de expressões como $8 = 2 + 3 + 3$? Como dar continuidade a essa atividade para outra que pede todas as decomposições de 8? O que você acha que a criança aprende com esse tipo de atividade? Pode ser feito um esquema similar para decomposições multiplicativas?

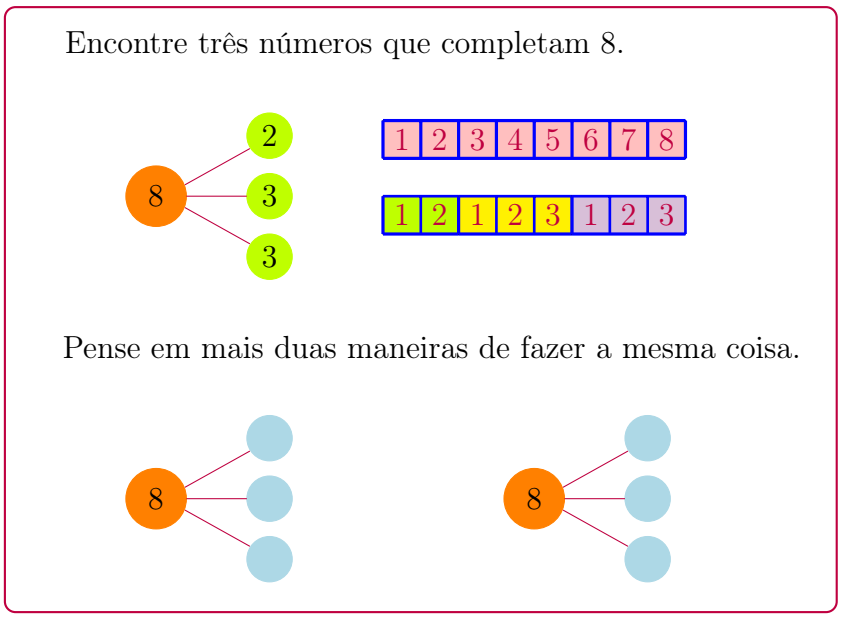



Figura 3.5. Esquema de atividade para o aprendizado de decomposições aditivas de números.

**Atividade 3.10.8.** Em expressões aritméticas envolvendo várias operações, não existe, do ponto de vista lógico, uma ordem preferencial sobre qual cálculo deve ser feito primeiro. A "Matemática" não estabelece sobre isso regra alguma. Autores de textos ou aplicativos devem deixar claro que regra seguem. Na ausência de regras a ordem de cálculo deve ser determinada pelo uso de separadores, como parêntesis, colchetes ou chaves. (i) Na internet vemos vídeos pedindo o resultado de expressões em que não se usa separadores. Analise alguns desses vídeos. (ii) Um estudante, pretendendo resolver essa questão, estabeleceu a seguinte regra: em uma expressão aritmética sem separadores, deve-se calcular as operações na seguinte ordem: potenciação, divisão, multiplicação, subtração e adição. Isso resolve? (iii) Um professor estabeleceu o seguinte: em expressões aritméticas sem parêntesis, colchetes ou chaves, as operações de multiplicação e divisão têm prioridade sobre as de soma e subtração. Isso resolve?

## 3.11 Temas para investigação

**Tema 3.11.1.** Investigue o seguinte problema. Dados números naturais, um com $n$ dígitos e outro com $m$ dígitos, quantos dígitos tem: **a)** sua soma; **b)** sua diferença; **c)** seu produto; **d)** o quociente e o resto da divisão do maior pelo menor.

**Tema 3.11.2.** Considerando o sistema de numeração decimal e o Problema 2.5.18, caracterize os números naturais que, somados com seu reverso, resulta em um múltiplo de 11. E quanto a sistemas em outras bases?

**Tema 3.11.3.** Tome um número e seu reverso. Subtraia o menor do maior. Tome o resultado e repita o processo. Repita se achar necessário. O que acontece?

**Tema 3.11.4.** Investigue se um resultado análogo ao do Problema 3.9.13 funciona para outras bases e outras potências.

**Tema 3.11.5.** Um número natural $n$ de dois dígitos (portanto $10 \leq n \leq 99$) é denominado *supernúmero* se $n$ é a soma $n = a + b$ de números naturais $a$ e $b$, cada um com dois dígitos, e se a soma dos dígitos de $n$ é igual à soma conjunta dos dígitos de $a$ e de $b$.

Investigue quem são os supernúmeros $n$ e como são as parcelas $a$ e $b$ tais que $n = a + b$ nas condições dadas.

Dado um supernúmero $n$, as decomposições $n = a + b$ e $n = b + a$ são consideradas iguais. Determine quantas decomposições diferentes tem $n$.

Investigue o que ocorre com números com um dígito, três dígitos, etc.

**Tema 3.11.6.** Chamamos de *operação unitária* a uma adição ou multiplicação de dois algarismos decimais quaisquer. **a)** Dados números naturais $a$ e $b$ representados no sistema decimal, seja $A(a, b)$ a quantidade de operações unitárias necessárias para somar $a$ e $b$ usando o algoritmo usual. Encontre uma cota superior para $A(a, b)$ em função do número de dígitos de $a$ e de $b$. Isto é, encontre um número $c(n, m)$ tal que $A(a, b) \leq c(n, m)$, sendo $n$ o número de dígitos de $a$ e $m$ o número de dígitos de $b$. **b)** Dados números naturais $a$ e $b$ representados no sistema decimal, seja $M(a, b)$ a quantidade de operações unitárias necessárias para multiplicar $a$ e $b$ usando o algoritmo usual. Encontre uma cota superior para $M(a, b)$ em função do número de dígitos de $a$ e de $b$.

**Tema 3.11.7.** Tome um número de quatro dígitos, não todos iguais. Rearranjando os dígitos coloque-os em ordem decrescente, e depois em ordem crescente (isto é, tome o maior e o menor dentre os números que podem ser escritos com os dígitos do número considerado inicialmente). Subtraia o menor do maior. Encontre um número invariante quando submetido a esse procedimento. O que ocorre com outros números se aplicarmos o procedimento sucessivamente? O que ocorre com números com dois dígitos? Com três? Alguma generalização?

**Tema 3.11.8.** Investigue se é possível construir táboas para as operações de adição e de multiplicação para o sistema fatorial, definido na página 34.

**Tema 3.11.9.** Defina sequências de números naturais da seguinte forma. Dado um número natural $n$, o elemento seguinte da sequência é a soma dos quadrados dos dígitos da representação decimal de $n$. E assim sucessivamente. Por exemplo,

$$55 \to 50 \to 25 \to 29 \quad \ldots$$

Estude o comportamento dessas sequências.

**Tema 3.11.10.** No sistema decimal, somando-se um número natural de dois dígitos ou mais com seu reverso, e repetindo esse procedimento várias vezes se necessário, eventualmente se obtém um número palíndromo, ou capicua. Faça alguns testes. Como se pode demonstrar que esse fenômeno ocorre para todo número com dois dígitos? O que significa um contra-exemplo para essa propriedade? Pesquise na internet os termos "lychrel number" e "196-algorithm". O que ocorre em sistemas de numeração em bases não decimais?

**Tema 3.11.11.** Para analisar a relação entre os números naturais $a$ e $b$, podemos dividir o maior pelo menor. Conforme já observamos, se $a = bq$ dizemos que $a$ é múltiplo que $b$, e isso é bom pois facilita muitos cálculos. Mas, se $a = bq + r$, vemos que esse resto, por assim dizer, atrapalha. Uma ideia que os antigos matemáticos gregos tiveram foi continuar a divisão. Supondo que $r < b$, dividimos $b$ por $r$. Podemos repetir esse procedimento tantas vezes quanto for possível. Faça vários exemplos e investigue as propriedades dessa sequência de divisões.

# Parte II

# Introdução à teoria dos números naturais

# Capítulo 4

# O ideal matemático da Antiga Grécia

## 4.1 Introdução

A antiga civilização grega, particularmente a do Período Arcaico (776 a 323 a.C.), é considerada a origem da atual civilização ocidental. Manifestou os ideais filosóficos, científicos, políticos, sociais e artísticos que tiveram influência decisiva no mundo ocidental.

A Matemática, vista como ciência dedutiva, começou a ser desenvolvida nesse período. Antes dos gregos os estudiosos egípcios, sumérios, hindus e persas investigavam os números e as formas geométricas através de um senso estético. Os matemáticos gregos conservaram a beleza mas a transformaram completamente, criando uma ciência dedutiva, com definições, postulados, axiomas e teoremas. Confira [122], página XI.

Distinguiram-se, dentre muitos estudiosos, os discípulos das Escolas Pitagórica e Platônica, que se dedicaram ao estudo das figuras e números usando métodos de análise e dedução. Sobre Pitágoras de Samos afirma Proclus Diadochus, filósofo e historiador da Matemática, que ele transformou o estudo da Geometria em uma arte livre, examinando os princípios dessa ciência desde sua gênese. Aristoxenus de Tarento, filósofo grego do século IV a.C., afirma ainda que Pitágoras dava muita importância ao estudo da Aritmética, em que promoveu grandes avanços, desvinculando-a de suas aplicações comerciais. Confira [48], página 37. Os resultados matemáticos obtidos nesse período foram organizados na famosa coleção de livros *Os Elementos*, escrita por Euclides em Alexandria por volta de 300 a.C.

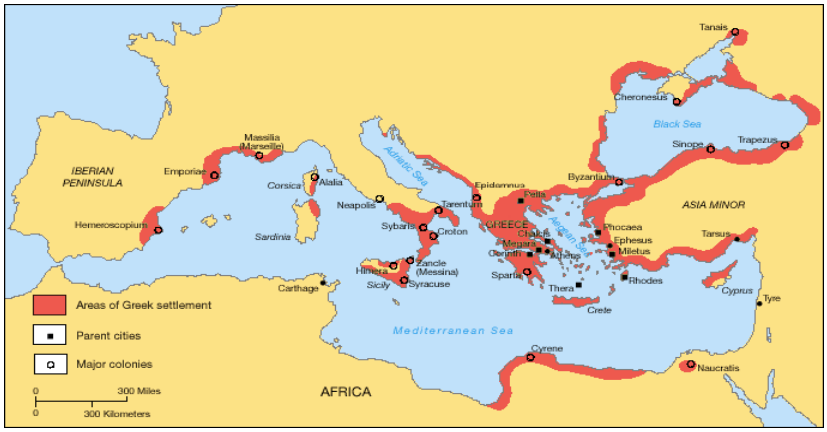



Figura 4.1. No mapa estão indicados os territórios da Antiga Grécia no Período Arcaico (776 a 323 a.C.). Estão assinalados também os assentamentos gregos, as colônias e cidades coligadas.

Para iniciar nossos estudos em Teoria dos Números seguem alguns problemas sobre números naturais. O primeiro está resolvido.

**Problema resolvido 4.1.** Um estudante fez uma tabela com duas linhas e cem colunas. Na primeira linha escreveu os números naturais de 1 a 100 em sua ordem normal. Na segunda linha escreveu a letra $Q$ embaixo de todos os números que são quadrados de números naturais, e a letra $N$ embaixo dos outros.

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | ... | 100 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Q | N | N | Q | N | N | N | N | Q | N | N | N | N | N | N | Q | N | ... | Q |

**a)** Quantas vezes o estudante escreveu a letra $Q$ e quantas a letra $N$? **b)** Se a tabela continuasse indefinidamente, pergunta-se para que valores de $n$ haveriam sequências do tipo $QNN\ldots NQ$ com $n$ letras $N$ entre duas letras $Q$ subsequentes.

*Solução.* **a)** De 1 a 100 os quadrados de números naturais são $1^2 = 1$, $2^2 = 4$, ... $10^2 = 100$, portanto são dez. Dessa forma a letra $Q$ foi escrita dez vezes e a letra $N$, noventa. **b)** Entre um quadrado $m^2$ e seu consecutivo $(m+1)^2$ existem $(m+1)^2 - m^2 - 1 = 2m$ posições (excluindo as posições de $m^2$ e $(m+1)^2$ ). Então $n = 2m$ para todo número natural $m \geq 1$. □

## 4.2 Problemas

**Problema 4.2.1.** Consideremos os números naturais dispostos, em sua sequência normal, em linhas com cinco números em cada uma:

$$\begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ 6 & 7 & 8 & 9 & 10 \\ 11 & 12 & 13 & 14 & 15 \\ 16 & 17 & 18 & 19 & 20 \\ \vdots & \vdots & \vdots & \vdots & \vdots \end{array}$$

**a)** Pergunta-se em que linha a soma dos números que a compõem é igual a 665 (descreva quais são os números que fazem parte dessa linha e qual a posição da linha na sequência de linhas).
**b)** Se o problema foi resolvido, descreva o processo de descoberta. Analise se foi feita uma indução[1] ou uma dedução[2]. Considere se sua solução necessita de alguma justificativa algébrica, e elabore essa justificativa.
**c)** Imagine que você esteja trabalhando com uma classe de estudantes e resolve apresentar-lhes o problema acima. Você aceitaria como válida uma solução indutiva, ou exigiria uma solução dedutiva? Em que situações o professor deveria trabalhar com um ou outro caso?

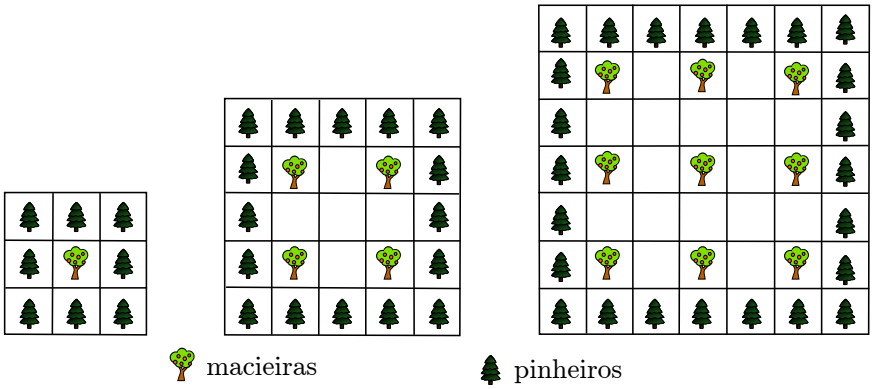
**Problema 4.2.2.** Consideremos os números naturais dispostos em linhas, em sua sequência normal, conforme descrito abaixo. Que propriedades podem ser observadas? Alguma demonstração?

[1] Indução: operação que estabelece uma proposição geral com base no conhecimento de um certo número de dados particulares.

[2] Dedução: operação que estabelece uma proposição geral com base em uma ou mais premissas com uma correta aplicação das regras da Lógica.

$$
\begin{array}{ccccccc}
 & & & 1 & & & \\
 & & 2 & 3 & 4 & & \\
 & 5 & 6 & 7 & 8 & 9 & \\
10 & 11 & 12 & 13 & \ldots & &
\end{array}
$$

**Problema 4.2.3.** Um fazendeiro planeja plantar macieiras em um terreno quadrado. Para protegê-las do vento pretende plantar pinheiros ao redor das macieiras. Desenhou três diagramas para estudo.



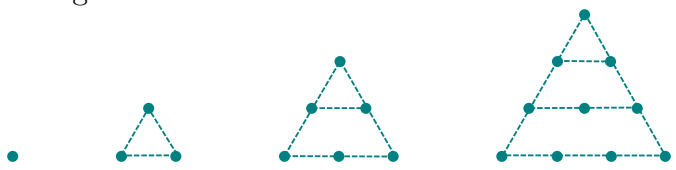

Tomando como unidade de medida o lado do quadradinho ocupado por uma planta, o fazendeiro necessita responder às seguintes questões: **a)** qual o lado do terreno necessário para plantar $k^2$ macieiras; **b)** quantos pinheiros são necessários para plantar $k^2$ macieiras; **c)** observando que nos diagramas acima a quantidade de pinheiros é maior do que a de macieiras, quais são os valores de $k$ para os quais essa situação se inverte? **d)** Para cada um dos itens resolvidos, você fez uma indução ou uma dedução?

## 4.3 Números e Geometria

O estudo dos números no tempo dos antigos gregos era fortemente influenciado pela Geometria, já que ela aglutina elementos mais concretos aos conceitos abstratos da Matemática. Dessa forma os números eram classificados de acordo com propriedades geométricas correspondentes, e números eram obtidos a partir de outros mediante manipulação de figuras.

Por exemplo, o produto de um número natural por outro era visto como a área de um retângulo, e particularmente o produto de um número natural por si mesmo era visto como a área de um quadrado. Os números assim gerados eram denominados planares. Da mesma forma o produto de três números naturais era denominado número sólido, sendo cubo o caso particular em que os três números são iguais. Em nossa linguagem matemática comum ainda guardamos essas relações, pois denominamos $a^2$ de "$a$ ao quadrado" e $a^3$ de "$a$ ao cubo".

Os antigos gregos também relacionavam números com figuras geométricas através de desenhos com pontos. Por exemplo, os números 1, 3, 6 e 10 correspondem, respectivamente, à quantidade de pontos nas figuras



e por isso eram denominados *números triangulares*. Evidentemente podemos continuar essa sequência de figuras e obter uma infinidade de números triangulares. A quantidade de pontos da $n$-ésima figura corresponde ao $n$-ésimo número triangular, que indicamos com a notação $T_n$. Dessas figuras vemos que $T_1 = 1$, $T_2 = 3$, $T_3 = 6$, e $T_4 = 10$.

Podemos encontrar uma expressão geral para $T_n$. Percebemos que a $n$-ésima figura é obtida da anterior mediante o acréscimo de uma linha com $n$ pontos. Começando com $T_1 = 1$ temos $T_2 = T_1 + 2 = 1 + 2$, depois $T_3 = T_2 + 3 = 1 + 2 + 3$, e $T_4 = T_3 + 4 = 1 + 2 + 3 + 4$.

Essas observações nos inspiram definir a sequência $T_n$ por

$$\begin{cases} T_1 &= 1, \\ T_n &= T_{n-1} + n \quad \text{para } n = 2, 3, \ldots \end{cases} \tag{4.1}$$

ou por

$$T_n = 1 + 2 + 3 + \cdots + n \quad \text{para todo número natural } n. \tag{4.2}$$

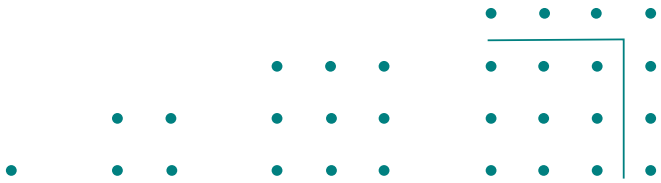
Nessa segunda definição entendemos que se $n = 1$ a soma $1 + 2 + 3 + \cdots + n$ significa 1.

Lembrando que $1+2+3+\cdots+n = n(n+1)/2$ (usando a fórmula da soma dos $n$ primeiros termos de uma progressão aritmética), podemos escrever ainda

$$T_n = \frac{n(n+1)}{2} \quad \text{para todo número natural } n. \tag{4.3}$$

No problema 4.4.2 abaixo o estudante é convidado a explorar as diferenças entre essas definições. A definição (4.1) chama-se *definição por recorrência*. Ela tem esse nome porque para obter o $n$-ésimo termo da sequência temos que recorrer ao $(n-1)$-ésimo. Já em (4.3) para obter o $n$-ésimo termo não necessitamos conhecer nenhum termo anterior.

A sequência dos números quadrados corresponde às figuras



Indicamos por $Q_n$ o $n$-ésimo número quadrado. Portanto $Q_n = n^2$ para todo número natural $n$. Assim cada número $Q_n$ corresponde a um quadrado formado por $n^2$ pontos.

Observando a lei de formação das figuras quadradas, notamos que cada figura é obtida da anterior mediante o acréscimo de um *gnômon*, figura da forma $\begin{matrix} \cdots \\ \vdots \end{matrix}$ contendo $2n-1$ pontos, conforme está sugerido no último quadrado da figura acima. Obtemos assim a definição por recorrência

$$\begin{cases} Q_1 &= 1, \\ Q_n &= Q_{n-1} + (2n-1) \quad \text{para } n = 2, 3, \ldots \end{cases}$$

Para conferir essa fórmula podemos ver que $Q_{n-1} + (2n-1) = (n-1)^2 + 2n - 1 = n^2 - 2n + 1 + 2n - 1 = n^2 = Q_n$.

Notemos as seguintes relações: $Q_1 = 1$, $Q_2 = 1 + 3$, $Q_3 = 1 + 3 + 5$, etc., das quais vemos que $Q_n$ é a soma dos $n$ primeiros números naturais ímpares:

$$1 + 3 + 5 + \cdots + (2n-1) = n^2 \quad \text{para todo número natural } n.$$

Essas propriedades eram conhecidas na Escola Pitagórica (confira [48], página 44). Os pitagóricos também consideravam em suas investigações os números pentagonais, os números hexagonais, etc. Esse processo se estendia para a dimensão três, com o estudo dos números poliedrais. A riqueza de combinações encontradas nessas sequências constituíam uma ilustração do aforismo pitagórico "Tudo é Número", uma das principais ideias daquela Escola.



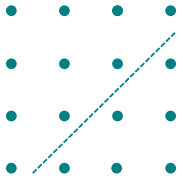
Figura 4.2. A Figura da esquerda é parte do celebrado quadro *Escola de Atenas*, de Rafael Sanzio, pintado de 1509 a 1510 na *Stanza della Segnatura* (Vaticano). Vemos a imagem de Pitágoras explicando sua teoria musical. O detalhe mostra a tableta com alguns símbolos musicais e o número triangular $1+2+3+4$, a sagrada *tetractys* dos pitagóricos.

## 4.4 Problemas

**Problema 4.4.1. a)** Seja $a_1$, $a_2$, ..., $a_n$ uma progressão aritmética com $n$ termos. Justifique a fórmula $a_1 + a_2 + \cdots + a_n = n(a_1 + a_n)/2$. **b)** Usando essa fórmula explique por que $1+2+3+\cdots+n = n(n+1)/2$ para todo número natural $n \geq 1$. **c)** Do mesmo modo expresse a soma $1 + 3 + 5 + \cdots + (2n-1)$ como uma fórmula, para todo número natural $n \geq 1$.

**Problema 4.4.2. a)** Calcule $T_{20}$ usando *i)* a definição por recorrência (4.1); *ii)* a definição por soma (4.2), e *iii)* a definição direta (4.3). Estude detalhadamente cada um desses métodos especificando as diferenças entre eles. **b)** Calcule $T_{1000}$ usando a forma menos dispendiosa.

**Problema 4.4.3.** A figura abaixo sugere uma relação geral entre números triangulares e quadrados. Descubra qual é a relação e demonstre-a usando recursos algébricos. Segundo o historiador Thomas L. Heath essa relação era conhecida dos antigos gregos (confira [48], página 50).



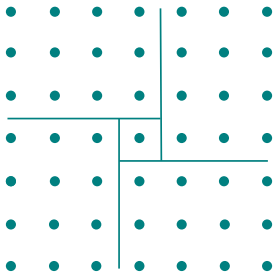
**Problema 4.4.4.** Os antigos gregos chamavam de *oblongos* os números da forma $n(n+1)$ (confira [48], página 49). As figuras relacionadas com esses números são os retângulos $n\times(n+1)$. Vemos abaixo a representação do número oblongo $4 \times 5 = 20$.



Utilizando figuras de números oblongos como inspiração, obtenha uma fórmula para a soma dos $n$ primeiros números naturais pares. Você fez uma indução ou uma dedução? Apresente uma demonstração algébrica da fórmula e constate sua validade para qualquer $n$.

**Problema 4.4.5.** Através de figuras verifique que os números oblongos podem ser escritos como soma de dois números triangulares iguais. Em seguida demonstre essa relação.

**Problema 4.4.6.** A figura abaixo e o problema anterior sugerem uma relação geral entre os números quadrados ímpares e números triangulares.



Descubra qual é a relação, descreva-a como uma fórmula, e demonstre-a.

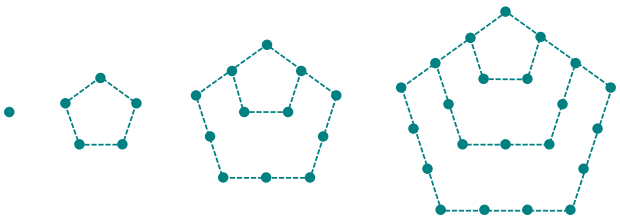
**Problema 4.4.7.** Leonard P. Euler observou que se $t$ é um número triangular então $9t + 1$, $25t + 3$ e $49t + 6$ também são. Demonstre essas afirmações. Alguma fórmula geral?



Figura 4.3. Foto de pintura de Leonard Paul Euler, matemático suiço que passou a maior parte de sua vida em universidades da Alemanha e da Rússia. Considerado um dos grandes mestres, contribuiu em muitas áreas da Matemática e da Física, como Teoria dos Números, Análise, Equações Diferenciais, Teoria dos Grafos, Geometria, Mecânica, Dinâmica dos Fluidos, Ótica, Astronomia e Teoria da Música.

**Problema 4.4.8.** Descubra uma fórmula para validar a seguinte afirmação: todo cubo $n^3$ de número natural $n \geq 2$ se escreve como diferença dos quadrados de dois números triangulares. Não se esqueça de demonstrar a fórmula. Para completar o caso $n = 1$ defina o número triangular $T_0 = 0$.

**Problema 4.4.9.** Considere a sequência dos números pentagonais $P_n$ descrita pelas figuras a seguir:



Observando a lei de formação dessas figuras, confira a seguinte definição por recorrência dos números pentagonais:

$$\begin{cases} P_1 &= 1, \\ P_n &= P_{n-1} + 3n - 2 \quad \text{para } n = 2, 3, \ldots \end{cases}$$

Temos também a fórmula

$$P_n = \frac{n(3n-1)}{2} \quad \text{para } n = 1, 2, 3, \ldots$$

**a)** Descreva a diferença entre essas duas fórmulas. Verifique se é possível deduzir a segunda fórmula da primeira. **b)** Demonstre que $P_n = 2T_{n-1} + T_n$, para todo número natural $n \geq 2$.

## 4.5 Zero e os números naturais

Nos capítulos anteriores estudamos os números naturais 1, 2, 3, 4, ... e consideramos zero um algarismo dos sistemas posicionais, definido para designar a casa vazia em representações de números. Convém agora considerarmos zero um número natural, de modo que possamos estender as propriedades desse conjunto. Tomar zero como um número natural também facilita o desenvolvimento de fórmulas e definições.

A ideia de conjunto vazio surge quando fazemos certas operações com conjuntos. Por exemplo, dado um conjunto, retiramos dele todos os seus elementos, do que resulta um conjunto vazio. Fazendo a interseção de dois conjuntos que não têm elementos em comum, vemos que essa interseção é um conjunto vazio.

Isso nos sugere estender os números utilizados para contagem, considerando a

**Definição 4.2.** Designamos por *zero* a quantidade de elementos em um conjunto vazio. Indicamos o número zero com o símbolo 0.

Dessa forma zero faz parte dos números utilizados para contagem, que passam a ser: 0, 1, 2, 3, ...

Se em um conjunto vazio colocamos um objeto temos um conjunto com um elemento. Assim $1+0=1$ ou $0+1=1$. Vemos que 1 é o sucessor de zero. Mais geralmente, se em um conjunto vazio colocamos $n$ elementos, ficamos com $n$ elementos no conjunto, ou seja, $0+n=n$. Por outro lado, se em um conjunto com $n$ elementos acrescentamos elemento nenhum, continuamos com um conjunto com $n$ elementos. Portanto $n+0=n$. Em síntese,

$$n + 0 = n = 0 + n \quad \text{para todo número natural } n. \tag{4.4}$$

Em particular, $0+0=0$. Vemos também que se de um conjunto com $n$ elementos retiramos $n$ elementos, ficamos com um conjunto com 0 elementos, isto é,

$$n - n = 0 \quad \text{para todo número natural } n. \tag{4.5}$$

Em particular, $0 - 0 = 0$. Como $1 - 1 = 0$, vemos que o antecessor de 1 é zero. Fazendo considerações análogas temos $n - 0 = n$ para todo número natural $n$.

Vimos anteriomente que $1 \times n$ significa tomar $n$ uma vez, $2 \times n$ significa tomar $n + n$, etc. Assim $0 \times n$ significa tomar $n$ nenhuma vez, e o mais lógico parece ser definir $0 \times n = 0$ para todo $n$. Por outro lado $n \times 0$ é $0 + 0 + \ldots + 0$, resultando novamente 0. Temos assim

$$n \times 0 = 0 = 0 \times n \quad \text{para todo número natural } n. \tag{4.6}$$

Em particular, $0 \times 0 = 0$.

Quanto à potenciação, retomando a definição dada na Seção 3.7, temos $0^n = 0$ para todo $n \geq 1$. Quanto a tomar o expoente zero, é mais conveniente definir $a^0 = 1$ para todo número natural $a \geq 1$, pois isso combina melhor nas fórmulas. Não definimos o símbolo $0^0$.

**Definição 4.3.** Indicamos por $\mathbb{N}$ o conjunto dos números naturais, incluindo o zero. Portanto

$$\mathbb{N} = \{0, 1, 2, 3, 4, \ldots\}.$$

Vimos que a propriedade comutativa da adição se estende para esse novo conjunto dos números naturais, e examinando as considerações feitas na página 52 vemos que a propriedade associativa da adição também se estende para esse novo conjunto. O mesmo ocorre para as propriedades comutativa e associativa da multiplicação e para a propriedade distributiva. Vemos também que $0 < 1$ e que as propriedades de ordem dadas na seção 3.4, se estendem para o conjunto $\mathbb{N}$.

**Definição 4.4.** Indicamos por $\mathbb{N}^*$ o conjunto dos números naturais excluído o zero, denominados *números naturais positivos*. Portanto

$$\mathbb{N}^* = \{1, 2, 3, 4, \ldots\}.$$



Já vimos que vários povos antigos usavam um símbolo para o zero com a finalidade de indicar a casa vazia em representações posicionais. Não é claro quando se iniciou a ideia de considerar zero como número. Mas isso certamente era feito na Índia a partir do Século VII por matemáticos como Brahmagupta, Mahavira e Bhaskara. Em um livro de Matemática elementar Mahavira escreve que "... um número multiplicado por zero é zero, e um número permanece o mesmo quando zero é subtraído dele". Para mais informações confira [87].

Destacamos agora a seguinte propriedade, denominada *Lei da Integridade*:

**Teorema 4.5.** *Se $a$ e $b$ são números naturais tais que $ab = 0$, então $a = 0$ ou $b = 0$.*

*Demonstração.* Vimos na definição de multiplicação, na página 68, que o produto de números naturais positivos é positivo. Portanto se $a$ é positivo e se $b$ é positivo, então $ab$ é positivo. Isso implica que se $ab = 0$ então $a = 0$ ou $b = 0$. □

**Problema resolvido 4.6.** Demonstre que se $a$ e $b$ são números naturais tais que $ab = 1$ então $a = b = 1$.

*Solução.* Se fosse $a = 0$ ou $b = 0$ teríamos $ab = 0$. Portanto $a \geq 1$ e $b \geq 1$. Se fosse $a > 1$ aplicaríamos a propriedade da compatibilidade entre a ordem e a multiplicação (página 69) e teríamos $a \cdot b > 1 \cdot b$. Isso implicaria $ab > 1$, o que não é possível. Portanto $a = 1$. De $ab = 1$ e $a = 1$ temos $b = 1$, o que termina a demonstração. □


THE

GANITA-SÂRA-SANGRAHA

OF

MAHAVIRACARYA

WITH

ENGLISH TRANSLATION AND NOTES

Figura 4.4. Mahavira, também chamado de Mahaviracharya (Mahavira, o professor) viveu na Índia no século nove. É autor do compêndio Ganita Sara Sangraha, o mais antigo texto dedicado inteiramente à Matemática, separando-a da Astronomia. Esse texto contém operações aritméticas, frações, regra de três, medida de áreas, e problemas diversos. O livro descreve detalhadamente um método para o cálculo do MMC (mínimo múltiplo comum). Mahavira descobriu identidades algébricas como $a^3 = a(a+b)(a-b)+b^2(a-b)+b^3$, fórmulas de combinatória, cálculo aproximado do perímetro e da área de elipses e cálculo da raiz cúbica. Distinguiu-se por usar o sistema posicional decimal e o zero como número.

À direita, digitalização da capa de uma versão de 1912, em inglês, do livro Ganita Sara Sangraha, traduzido do sânscrito.

## 4.6 Problemas

Resolva os problemas desta seção usando exclusivamente os conceitos e propriedades das operações aritméticas vistos no Capítulo 3 e os resultados da seção anterior.

**Problema 4.6.1.** Demonstre que se $a$ e $b$ são números naturais tais que $a+b=a$ então $b=0$.

**Problema 4.6.2.** Estude algumas fórmulas para ver por que é mais conveniente definir $a^0 = 1$ para todo $a \geq 1$.

**Problema 4.6.3.** Verifique que a propriedade "$n \times 0 = 0 = 0 \times n$ para todo número natural $n$" referida no texto pode ser deduzida de outras propriedades vistas anteriormente.

**Problema 4.6.4.** Demonstre que existe um único antecessor de 1, ou seja, é único o número 0 tal que $0+1=1$.

**Problema 4.6.5.** Demonstre que, para todo número natural $a$, se $a^2 = a$ então $a = 0$ ou $a = 1$.

**Problema 4.6.6.** (Lei do Cancelamento da Multiplicação) Demonstre que se $a$, $b$ e $c$ são números naturais tais que $c \neq 0$ e $ac = bc$, então $a = b$.

**Problema 4.6.7.** Enuncie corretamente e demonstre a propriedade de compatibilidade entre a ordem e a multiplicação em $\mathbb{N}$: se $a$, $b$ e $c$ são números naturais vale $a < b \Rightarrow ac < bc$ ?

**Problema 4.6.8.** Verifique que se $a = 0$ ou $b = 1$ então $ab = a$. Demonstre a sentença recíproca: se $a$ e $b$ são números naturais tais que $ab = a$ então $a = 0$ ou $b = 1$. Qual é a sentença negativa dessa recíproca? Ela também é verdadeira?

**Problema 4.6.9.** (i) Verifique que, para estender a fórmula $a^n a^m = a^{n+m}$ para $n = 0$, deve-se definir $a^0 = 1$, para todo número natural $a \geq 1$. (ii) Como $0^n = 0$ para todo $n \geq 1$, seria mais lógico definir $0^0 = 0$. Mostre que isso atrapalha a fórmula para expoentes negativos $a^{-n} = 1/a^n$.

## 4.7 Par e ímpar

*Ludere par impar.*[3]

É muito antiga a classificação dos números naturais em pares e ímpares e a aplicação dessa ideia nas mais diversas situações. Perde-se na noite dos tempos a origem do jogo de adivinhação *par ou ímpar?* com o uso de contas ou dos dedos das mãos. Na Antiga Grécia a Escola Pitagórica incluía a classificação dos números em pares e ímpares em sua cosmogonia numerológica. Atribuíam aos números pares qualidades femininas, e aos ímpares, qualidades masculinas. Nicômaco escreveu, por volta do ano 100, que os pitagóricos definiam número par como aquele que pode ser repartido em duas partes iguais, e os números ímpares como aqueles que não podem ([48], página 39).

Para dividir um número natural $n$ por 2 podemos agrupar duas a duas as unidades de $n$. Apenas um dos dois casos seguintes pode ocorrer: 1º) todas as unidades de $n$ são agrupadas duas a duas; 2º) todas as unidades menos uma são agrupadas duas a duas. Por exemplo,

$$\begin{aligned} 8 &= (1+1)+(1+1)+(1+1)+(1+1), \\ 9 &= (1+1)+(1+1)+(1+1)+(1+1)+1. \end{aligned}$$

Assim, $8 = 2 \cdot 4$ e $9 = 2 \cdot 4 + 1$.

Portanto, dado um número natural $n$ qualquer, temos $n = 2q$ ou $n = 2q + 1$ para algum número natural $q$. O número natural $q$ é a quantidade de grupos de duas unidades, e é designado por *quociente*. Se $n = 2q$, dizemos que 0 é o resto da divisão de $n$ por 2, e se $n = 2q + 1$, o resto é 1. No caso em que $n = 0$, temos $n = 2 \cdot 0$, portanto 0 é da forma $0 = 2q$, com $q = 0$, e o resto da divisão de 0 por 2 é 0.

Em síntese, temos o

**Teorema 4.7.** *Todo número natural $n$ se escreve em uma e apenas uma das formas*

$$n = 2q \quad ou \quad n = 2q + 1,$$

*sendo $q$ um número natural.*

Os números naturais da forma $2q$, sendo $q$ um número natural, são chamados *múltiplos de 2*. Os números naturais da forma $2q + 1$ não são múltiplos de 2. Temos também a

**Definição 4.8.** Chamamos de *par* a todo número natural da forma $2q$ para algum número natural $q$, isto é, a números que têm resto zero quando divididos por 2. Chamamos de *ímpar* a todo número natural da forma $2q + 1$ para algum número natural $q$, isto é, a números que têm resto 1 quando divididos por 2.

Portanto, o conjunto dos números naturais fica particionado em dois subconjuntos disjuntos: os pares e os ímpares, chamados *classes de restos de dois* ou de *classes módulo dois*.



Figura 4.5. Foto de estátua de Nicômaco de Gerasa, situada na cidade de Nuremberg, Alemanha. Nicômaco é autor da obra *Introdução à Aritmética*, escrita por volta do ano 100, em que aborda os números pares e ímpares, os primos, os compostos e os números perfeitos e amigos. Apresenta descrição algébrica dos resultados, desvinculando a Teoria dos Números da Geometria.

[3] "Jogar par e ímpar". Horácio. Adaptado de [113], página 16.

**Definição 4.9.** Dizemos que os números naturais $a$ e $b$ *têm a mesma paridade* se forem ambos pares ou ambos ímpares. Caso contrário, dizemos que *têm paridade oposta.*

Em outros termos, dizemos que dois números naturais têm a mesma paridade se estiverem na mesma classe módulo dois, e que têm paridade oposta se estiverem em classes diferentes. Por exemplo, 21 e 29 têm a mesma paridade, assim como 32 e 54. Mas 35 e 42 têm paridade oposta.

Podemos observar diversas propriedades dos números pares e ímpares. Por exemplo, $6+12 = 18$, $8 + 34 = 42$, etc. o que parece indicar que a soma de dois números naturais pares é sempre par. Também parece ser sempre par a soma de dois números naturais ímpares, como atestam os exemplos $7 + 9 = 16$, $13 + 19 = 32$. Por outro lado, $8 + 13 = 21$, $18 + 35 = 53$, etc. o que parece indicar que a soma de um par com um ímpar é sempre ímpar. Usando notação algébrica obtemos resultados gerais, conforme a

**Proposição 4.10.** *A soma (ou diferença) de dois números naturais de mesma paridade é par. A soma (ou diferença) de dois números naturais de paridade oposta é ímpar.*

*Demonstração.* Vejamos as afirmações sobre a soma (sobre a diferença fica como exercício para o estudante no Problema 4.8.2). Sejam $a$ e $b$ números naturais de mesma paridade. Suponhamos primeiro que sejam ambos pares. Então existem números naturais $n$ e $m$ tais que $a = 2n$ e $b = 2m$. Temos $a + b = 2n + 2m = 2(n + m) = 2t$, com $t = n + m$. Como $t$ é um número natural, segue que $a + b$ é par. Suponhamos agora que $a$ e $b$ sejam ambos ímpares. Podemos escrever $a = 2n + 1$ e $b = 2m + 1$, sendo $n$ e $m$ números naturais. Então $a+b = 2n+1+2m+1 = 2(n+m+1) = 2t$, com $t = n+m+1$. Como $t$ é um número natural, segue que $a + b$ é par. Portanto a soma de dois números de mesma paridade é par.

Sejam agora $a$ e $b$ números naturais de paridade oposta. Sem perda de generalidade podemos supor que $a$ é par e $b$ ímpar. Então existem números naturais $n$ e $m$ tais que $a = 2n$ e $b = 2m+1$. Assim $a + b = 2n + 2m + 1 = 2(n + m) + 1$, e $a + b$ é ímpar. Portanto a soma de dois números de paridade oposta é ímpar. □

Consideremos uma tabela dos números pares e ímpares representados no sistema decimal:

| pares | ímpares |
|---|---|
| 0 | 1 |
| 2 | 3 |
| 4 | 5 |
| 6 | 7 |
| 8 | 9 |
| 10 | 11 |
| 12 | 13 |
| 14 | 15 |
| 16 | 17 |
| 18 | 19 |
| 20 | 21 |

Podemos notar várias propriedades. Por exemplo, um número e seu quadrado parecem estar sempre na mesma classe. Para confirmar fazemos a

**Proposição 4.11.** *Todo número natural e seu quadrado têm a mesma paridade. Em outros termos, todo número natural e seu quadrado estão na mesma classe módulo dois.*

*Demonstração.* De fato, se $n = 2q+1$, então $n^2 = (2q+1)^2 = 4q^2+4q+1 = 2(2q^2+2q)+1 = 2l+1$, sendo $l$ um número natural. Portanto, se $n$ é ímpar, $n^2$ também o é. Por outro lado, se $n = 2q$, então $n^2 = 4q^2 = 2(2q^2) = 2l$. Em consequência, se $n$ é par, $n^2$ também é par.

Reciprocamente, se $n^2$ é par, então $n$ não pode ser ímpar, pois se o fosse $n^2$ seria ímpar, em virtude da conclusão acima. Portanto se $n^2$ é par então $n$ é par. Por outro lado, se $n^2$ é ímpar, então $n$ não pode ser par, pois se o fosse $n^2$ seria par, em virtude da conclusão acima. Portanto se $n^2$ é ímpar então $n$ é ímpar. □

Vemos que a demonstração dessa proposição usa fortemente a dicotomia imposta aos números naturais pela sua classificação módulo dois: dado qualquer número natural, ele **ou** é par, **ou** é ímpar.

**Definição 4.12.** Um número natural diz-se ser um *quadrado perfeito* se for quadrado de um número natural.

Por exemplo, 16 é um quadrado perfeito, pois $16 = 4^2$.

A Proposição 4.11 pode ser enunciada da seguinte forma: *Todo quadrado perfeito e sua raiz quadrada têm a mesma paridade.*

Observando novamente a tabela acima de pares e ímpares, notamos outra propriedade, bastante conhecida:

**Proposição 4.13.** *O número natural $n$ é par quando o dígito das unidades de sua representação decimal é par.*

Essa propriedade chama-se *critério de divisibilidade por* 2. O que mais nos chama a atenção nesse critério é sua utilidade e simplicidade de aplicação. Assim, para sabermos que o número 938 740 816 é par, não é necessário dividi-lo por 2. Basta olhar para o dígito das unidades.

*Demonstração.* Para demonstrar o critério de divisibilidade por 2, vamos primeiro enunciá-lo da seguinte forma:

$$n = (a_m \dots a_1 a_0)_{\text{dez}} \text{ é par se e somente se } a_0 \text{ é par.}$$

Observemos que

$$\begin{aligned} n &= a_m 10^m + \ldots + a_1 10 + a_0 \\ &= 2a + a_0 \end{aligned}$$

para um certo número natural $a$. Assim, se $n$ é par, $a_0 = n - 2a$ também é par, como diferença de dois pares. Reciprocamente, se $a_0$ é par, então $n = 2a + a_0$ é par, como soma de dois pares. Isso demonstra o critério. □

Uma consequência do critério acima é que $n = (a_m \dots a_0)_{\text{dez}}$ é ímpar se e somente se $a_0$ é ímpar. Em resumo, um número natural qualquer e seu dígito decimal das unidades têm a mesma paridade.

O conceito de par e ímpar pode ser utilizado para resolver problemas que dependem dessa partição do conjunto dos números naturais. Por exemplo,

**Problema resolvido 4.14.** (confira [123], página 11) Em um quartel existem 100 soldados e, todas as noites, três deles são escolhidos para trabalhar de sentinela. É possível que após certo tempo um dos soldados tenha trabalhado com cada um dos outros exatamente uma vez?

*Solução.* Não é possível. Fixemos um dos soldados. Seus 99 companheiros podem formar 49 grupos de dois soldados, e sobra 1, pois $99 = 2 \times 49 + 1$. Assim em 49 noites o soldado fixado pode ficar de sentinela com dois companheiros, sendo sempre companheiros diferentes. Mas na 50ª. noite esse companheiro que sobrou vai ter que se juntar a outro que já fez sentinela com o soldado fixado inicialmente. □

**Problema resolvido 4.15.** (confira [123], página 14) Um tabuleiro de xadrez $6\times6$ está coberto com dominós $2\times1$ (confira definição de tabuleiro de xadrez no Problema 4.8.19 abaixo). Mostre que existe uma reta que separa as peças do tabuleiro sem cortar nenhum dominó, qualquer que seja a distribução dos dominós.

*Solução.* As retas que separam as casas do tabuleiro são horizontais ou verticais, e são em número de 10. Mostraremos primeiro que se uma reta que separa casas do tabuleiro corta um dominó, então corta pelo menos dois. De fato, digamos que uma dessas retas corta exatamente um dominó. Então de um dos lados da reta existem $n$ dominós inteiros e mais $1/2$ dominó. Portanto desse lado da reta existem $2n+1$ casas do tabuleiro. Mas isso não é possível, pois essa parte do tabuleiro é formada por linhas (ou colunas) completas com 6 casas cada, assim tem um número par de casas. Portanto, se cada uma das 10 retas que separam casas do tabuleiro corta um dominó, então cada uma dessas retas corta pelo menos dois dominós, todos diferentes. Assim essas 10 retas determinam 20 dominós, pelo menos. Mas, como o tabuleiro tem 36 casas, existem 18 dominós cobrindo todas as casas. Temos assim uma contradição, advinda do fato de termos admitido que todas as 10 retas cortam algum dominó. Em consequência pelo menos uma das 10 retas não corta dominó algum. □

Usamos divisão por 2 para classificar os números naturais em pares e ímpares. O que ocorre se usarmos divisão por 3? Dado $n$, repartimos suas unidades na maior quantidade possível de grupos de três unidades. Os restos possíveis são: 0 ou 1 ou 2. Portanto, todo número natural $n$ é de uma e apenas uma das seguintes formas:

$$n = 3q \quad \text{ou} \quad n = 3q + 1 \quad \text{ou} \quad n = 3q + 2$$

para algum número natural $q$.

Vemos assim que o conjunto dos números naturais se particiona nos três subconjuntos seguintes, chamados *classes de restos de três* ou *classes módulo três*:

| resto zero | resto um | resto dois |
|---|---|---|
| 0 | 1 | 2 |
| 3 | 4 | 5 |
| 6 | 7 | 8 |
| 9 | 10 | 11 |
| 12 | 13 | 14 |
| 15 | 16 | 17 |
| 18 | 19 | 20 |
| 21 | 22 | 23 |
| 24 | 25 | 26 |
| ⋮ | ⋮ | ⋮ |

Na primeira coluna estão os números que têm resto zero quando divididos por três. Dizemos que esses números são *múltiplos de 3*. Na segunda coluna, os que têm resto um, e na terceira, resto dois.

Existem, como vimos, duas classes de números naturais módulo dois: os pares e os ímpares. A literatura matemática não consagrou nomes para as classes módulo três. A turma de 1995 do Curso de Matemática da Universidade Federal de São Carlos (UFSCar) sugeriu a seguinte nomenclatura:

| | |
|---|---|
| ter | (para números da forma $3q$); |
| ínter | (para números da forma $3q+1$); |
| alter | (para números da forma $3q+2$). |

Podemos usar as classes módulo três para demonstrar propriedades relacionadas com essa partição. Por exemplo,

**Problema resolvido 4.16.** Dados três números naturais consecutivos quaisquer, exatamente um deles é múltiplo de 3.

*1ª. solução.* Sejam $a$, $a+1$ e $a+2$ números naturais consecutivos. A situação nos sugere considerar classes módulo três. Como $a$ está em exatamente uma dessas classes, temos três casos a considerar: *i)* $a = 3q$, ou *ii)* $a = 3q+1$, ou *iii)* $a = 3q+2$, para algum número natural $q$. Devemos examinar o que ocorre em cada um desses casos. Vejamos.

*i)* $a = 3q$ para algum número natural $q$. Então $a+1 = 3q+1$ e $a+2 = 3q+2$. Portanto $a$ é múltiplo de 3 e $a+1$ e $a+2$ não são.

*ii)* $a = 3q+1$ para algum número natural $q$. Então $a+1 = 3q+2$ e $a+2 = 3q+3 = 3(q+1)$. Portanto $a+2$ é múltiplo de 3 e $a$ e $a+1$ não são.

*iii)* $a = 3q+2$ para algum número natural $q$. Então $a+1 = 3q+3 = 3(q+1)$ e $a+2 = 3q+4 = 3(q+1)+1$. Portanto $a+1$ é múltiplo de 3 e $a$ e $a+2$ não são.

*2ª. solução.* Os múltiplos de 3 são 3, 6, 9, ..., e formam assim uma progressão aritmética de razão 3. Dados dois números consecutivos $3q$ e $3(q+1) = 3q+3$ dessa sequência, vemos que entre eles existem apenas dois números naturais, a saber, $3q+1$ e $3q+2$. Portanto, dados três números naturais consecutivos, exatamente um deles pertence à referida progressão. □

**Problema resolvido 4.17.** Mostre que $m$ é múltiplo de 3 se e somente se $m^2$ também é múltiplo de 3.

*Solução.* Se $m$ é múltiplo de 3 então $m$ se escreve na forma $m = 3k$ para algum número natural $k$. Portanto $m^2 = 9k^2 = 3(3k^2)$ também é múltiplo de 3.

Vejamos a recíproca. Suponhamos que $m^2$ seja múltiplo de 3. O número $m$ pertence a uma das classes módulo três. Portanto temos três possibilidades: $m = 3q$ ou $m = 3q+1$ ou $m = 3q+2$, para algum número natural $q$. Se $m$ é da forma $m = 3q+1$, então $m^2 = (3q+1)^2 = 9q^2+6q+1 = 3(3q^2+2q)+1$, e $m^2$ não é múltiplo de 3. Por outro lado, se $m$ é da forma $m = 3q+2$, então $m^2 = (3q+2)^2 = 9q^2+12q+4 = 9q^2+12q+3+1 = 3(3q^2+4q+1)+1$, e $m^2$ novamente não é múltiplo de 3. Constatamos assim que $m$ não pode ser da forma $3q+1$ e nem $3q+2$. Só resta a possibilidade de que $m = 3q$, e assim $m$ deve ser múltiplo de 3. □

De modo análogo ao que fizemos para 2 e 3 podemos considerar as *classes de restos de quatro* ou as *classes módulo quatro*. Dividindo um número natural por 4, os restos possíveis são 0 ou 1 ou 2 ou 3. Dessa forma o conjunto dos números naturais fica particionado em quatro subconjuntos disjuntos: o primeiro formado pelos números da forma $n = 4q$, o segundo pelos números da forma $n = 4q+1$, o terceiro pelos números da forma $n = 4q+2$ e o quarto pelos números da forma $n = 4q+3$.

Se o resto da divisão de um número natural por 4 for zero, dizemos que o número é *múltiplo* de 4.

E assim sucessivamente podemos considerar classes módulo $m$ para todo número natural $m \geq 2$. Essa ideia é a base da maioria das técnicas de investigação na Teoria dos Números.

## 4.8 Problemas

**Problema 4.8.1.** Foi escrito no texto que os pitagóricos definiam número par como aquele que pode ser repartido em duas partes iguais, e os números ímpares como aqueles que não podem. Essa definição coincide com a atual Definição 4.8? Podem-se deduzir as mesmas propriedades de ambas as definições?

**Problema 4.8.2.** Explique por que a diferença de dois números naturais de mesma paridade é par. Justifique ainda por que a diferença de dois números naturais de paridade oposta é ímpar.

**Problema 4.8.3.** Explique por que se um número natural é par, seu sucessor é ímpar, e vice-versa.

**Problema 4.8.4.** Sejam $n_1$, $n_2$, ..., $n_s$ números naturais que podem ser todos pares, ou apenas alguns, ou nenhum. Qual é a paridade da soma $n_1 + n_2 + \cdots + n_s$ ?

**Problema 4.8.5.** Verifique se é par ou ímpar, e justifique: **a)** o produto de dois números naturais de mesma paridade; **b)** o produto de dois números naturais de paridade oposta; **c)** o produto de $s$ números naturais pares; **d)** o produto de $s$ números naturais ímpares. **e)** o produto de $s$ números naturais, sendo alguns deles pares e os outros ímpares.

**Problema 4.8.6.** Explique por que, qualquer que seja o número natural $n$, ele e seu cubo têm a mesma paridade.

**Problema 4.8.7.** Explique por que, se $n^2$ é múltiplo de 3, também é múltiplo de 9, isto é, se escreve na forma $9q$ para algum número natural $q$.

**Problema 4.8.8.** Observe regularidades na seguinte sequência de eventos:

$$1 \cdot 5 = 5,\ \ 3 \cdot 5 = 15,\ \ 5 \cdot 5 = 25,\ \ 7 \cdot 5 = 35,\ \ 9 \cdot 5 = 55,\ \ 11 \cdot 5 = 55, ...$$

Faça conjecturas que sejam verdadeiras (pelo menos duas).

**Problema 4.8.9.** Sejam $n_1$, $n_2$, ..., $n_s$ números naturais representados no sistema decimal. Explique por que para que o produto $n_1 n_2 \cdots n_s$ termine em 5 é necessário e suficiente que pelo menos um dos números termine em 5 e todos os outros sejam ímpares.

*Solução.* Para mostrar que a condição é necessária, suponhamos que o produto $n_1 n_2 \cdots n_s$ termine em 5. Devemos provar que pelo menos um dos números termina em 5 e todos os outros são ímpares. Como o produto termina em 5, esse produto é ímpar, e já vimos que todos os números $n_j$ devem ser ímpares. Olhando a tábua de multiplicação dos algarismos, vemos que para que o produto de dois deles termine em 5 é necessário que pelo menos um deles seja 5. Assim sendo, pelo menos um dos números $n_j$ deve terminar em 5. Demonstramos que a condição é necessária.

Vamos mostrar que a condição dada é suficiente. Suponhamos que pelo menos um dos números termine em 5 e todos os outros sejam ímpares. Sem perda de generalidade podemos supor que $n_1$ termina em 5 e os outros são ímpares. Escrevemos $n_1$ na forma $n_1 = 10q + 5$. Por outro lado, o produto $n_2 n_3 \cdots n_s$ é ímpar, digamos $2k+1$. Logo $n_1 n_2 \cdots n_s = (10q+5)(2k+1) = 20qk + 10q + 10k + 5 = 10l + 5$, que termina em 5. Demonstramos que a condição é suficiente. □

**Problema 4.8.10.** Sejam $n_1$, $n_2$, ..., $n_s$ números naturais representados no sistema decimal. Determine (e justifique) condições necessárias e suficientes para que seu produto termine em zero.

**Problema 4.8.11.** Justifique por que, quaisquer que sejam os números naturais $a$ e $b$, se $a$ é ímpar então $b$ e $ab$ têm a mesma paridade. E se $a$ for par?

**Problema 4.8.12.** Explique por que o produto de três números naturais consecutivos quaisquer é múltiplo de 3. E quanto à soma?

**Problema 4.8.13.** Verifique se é par ou ímpar a diferença de dois números cúbicos consecutivos quaisquer. Justifique. Um número chama-se *cúbico* quando é da forma $n^3$ para algum número natural $n$.

**Problema 4.8.14.** Verifique a paridade de $(100)_{três}$ (verificar a paridade significa ver se é par ou ímpar).

**Problema 4.8.15.** Em um livro o autor pede para provar que se $a$ é ímpar e múltiplo de 3 então $a^2 - 1$ é múltiplo de 4. Verifique que uma das hipóteses sobre $a$ não é necessária para a validade da afirmação.

**Problema 4.8.16.** Determine a forma geral dos números naturais que são ao mesmo tempo ímpares e múltiplos de 3. E quanto aos pares múltiplos de 3?

**Problema 4.8.17.** Dizemos que um número natural $a$ é múltiplo de 8 quando ele se escreve na forma $a = 8q$ para algum número natural $q$. Encontre condições necessárias e suficientes sobre o número natural $n$ para que $n^2 - 1$ seja múltiplo de 8.

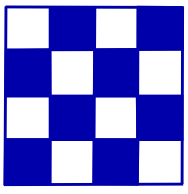
**Problema 4.8.18.** Determine o dígito da unidade do número

$$N = 1 \cdot 3 \cdot 5 \cdot 7 \cdot \ldots \cdot 2007$$

produto dos ímpares de 1 a 2007.

**Problema 4.8.19.** Um *tabuleiro retangular de xadrez* $m \times n$ consiste de um retângulo $m \times n$ quadriculado por $mn$ quadrados, chamados *casas*, pintados de branco e preto alternadamente nos sentidos vertical e horizontal. Um dia alguém mostrou a um estudante de Matemática um grande tabuleiro de xadrez, e afirmou: — aqui existem 484 casas. Olhando para o tabuleiro, e sem contar nada, o estudante replicou prontamente: — aqui não existem 484 casas. O que o estudante pode ter visualizado no tabuleiro que o levou a fazer essa afirmação tão prontamente?

Figura 4.6. Tabuleiro de xadrez $4 \times 4$.



**Problema 4.8.20.** Explique por que para todo número natural $n$ exatamente um dos números $n$, $n + 2$ ou $n + 4$ é múltiplo de 3.

**Problema 4.8.21.** Dados cinco números naturais quaisquer, sempre é possível escolher, dentre eles, três números cuja soma seja múltiplo de 3.

**Problema 4.8.22.** Investigue propriedades das classes módulo três. Faça afirmações gerais e justifique. Exemplos: O produto de dois números da mesma classe permanece nessa classe? Todo número natural e seu quadrado estão na mesma classe módulo três? Em que classes módulo três estão os quadrados perfeitos? Em que classes módulo três estão os números da forma $111\ldots1$ ($n$ 1's)?

**Problema 4.8.23.** Foi provado que o produto de dois ímpares é ímpar. Explique por que isso implica a seguinte afirmação: "Se 2 é fator do produto $ab$ então 2 é fator de $a$ ou de $b$". Mostre que essa afirmação também vale para 3, isto é: "Se 3 é fator do produto $ab$ então 3 é fator de $a$ ou de $b$". Vale o mesmo para 4?

**Problema 4.8.24.** Investigue propriedades das classes módulo quatro. Faça afirmações gerais e justifique. Em que classes módulo quatro estão os quadrados perfeitos? Em que classes módulo quatro estão os números da forma $111\ldots1$ ($n$ 1's)?

**Problema 4.8.25.** Construa uma tabela mostrando a partição do conjunto dos números naturais em classes módulo cinco. Observe por inspeção da tabela em que classes estão as potências quárticas dos números naturais. Faça uma conjectura geral e demonstre.

**Problema 4.8.26.** Em um jogo, dado um número natural $n$ é permitido realizar com ele uma das seguintes operações: *i)* substituí-lo pela sua metade se for par; *ii)* se o número for maior do que 1, subtrair 2 e substituí-lo pelo resultado.
**a)** Iniciando com um número natural $n$ e aplicando sucessivamente o procedimento *i)* acima tantas vezes quantas for possível, para que valores de $n$ se pode obter zero como valor final?
**b)** Mesma pergunta, mas agora com o procedimento *ii)*.

## 4.9 Análise dos números naturais

A *análise* é um recurso de investigação classificado pela teoria do conhecimento como um método que estuda os fenômenos decompondo-os em suas partes fundamentais, verificando como são construídos pela combinação dessas partes e examinando as relações entre os fenômenos através das interações entre essas partes.

Essa mesma ideia é aplicada no estudo dos números naturais. Nós os analisamos usando decomposição multiplicativa. Esse método deu origem à Teoria dos Números, iniciada por Pitágoras por volta de 500 a.C.

Observando a decomposição dos números naturais como produto de números $> 1$, vemos que alguns números podem assim se decompor, outros não. Os antigos gregos chamavam os primeiros de *planares*, e os outros de *retilíneos*. Hoje os denominamos respectivamente *números compostos* e *números primos*[4].

Exemplos de números compostos:

$$\begin{aligned} 12 &= 2 \times 6; \\ 15 &= 3 \times 5; \\ 117 &= 9 \times 13; \\ 392 &= 7 \times 56; \\ 539 &= 11 \times 49; \\ 2\,263\,261 &= 323 \times 7007. \end{aligned}$$

Exemplos de números que não se decompõem, portanto são primos:

$$2, \quad 3, \quad 5, \quad 7, \quad 11, \quad 13, \quad 17, \quad 19, \quad 503, \quad 809.$$

Convém formalizar algumas definições.

[4]Do latim *primu*, que significa primeiro.

**Definição 4.18.** Um número natural $a$ se diz *múltiplo* de um número natural $b$ se existir um número natural $q$ tal que $a = bq$. Nesse caso dizemos que $b$ é *fator* de $a$. Se $b \neq 0$, dizemos ainda que $b$ *divide* $a$ ou que $b$ é *divisor* de $a$; diz-se também que $a$ é *divisível* por $b$.

Lembramos que o termo *divisor* faz parte da nomenclatura da operação de divisão com significado similar.

Observamos que todo número natural $a$ é múltiplo de si mesmo e de 1, pois $a = 1 \cdot a$. Observamos ainda que 0 é múltiplo de qualquer número natural $a$, pois $0 = 0 \cdot a$, e que qualquer número natural $a \neq 0$ é divisor de 0.

**Definição 4.19.** Denominamos *primo* a todo número natural $> 1$ que não tem divisor diferente de 1 e dele mesmo. Chamamos de *composto* a todo número natural $> 1$ que tem divisor diferente de 1 e dele mesmo.

Observamos para os estudantes que já conhecem os números inteiros que, nesse ponto de nossos estudos, todos os fatores considerados são números naturais. Veremos os inteiros no Capítulo 9, quando consideramos também fatores negativos.

O número 1 não é composto e nem primo, assim como zero. Excluímos a unidade do conjunto de números primos por conveniência. Um dos motivos é o seguinte. Se desejamos afirmar que 6 se escreve de maneira única como produto de primos na forma $6 = 2 \times 3$ (desconsiderando a ordem do fatores), essa afirmação é possível graças ao fato de que 1 não é primo. Se o fosse, teríamos que considerar também as possibilidades $6 = 1 \times 2 \times 3$, $6 = 1 \times 1 \times 2 \times 3$, etc, o que seria bastante incômodo.

Uma propriedade simples mas importante é a seguinte:

**Proposição 4.20.** *Dados números naturais $a$, $b$ e $c$, se $a$ é múltiplo de $b$ e se $b$ é múltiplo de $c$, então $a$ é múltiplo de $c$.*

*Demonstração.* Existem números naturais $q$ e $t$ tais que $a = bq$ e $b = ct$. Portanto $a = bq = (ct)q = c(tq)$, e vemos que $a$ é múltiplo de $c$. □

Usando a nomenclatura da Definição 4.18 podemos reescrever o enunciado da Proposição 4.20 da seguinte forma: se $a$, $b \neq 0$ e $c \neq 0$ são números naturais tais que $c$ divide $b$ e $b$ divide $a$, então $c$ divide $a$.

Outra propriedade que convém destacar é a seguinte:

**Proposição 4.21.** *Dados números naturais $a$, $b$ e $c$, se $b$ e $c$ são múltiplos de $a$, então, quaisquer que sejam os números naturais $x$ e $y$, temos que $xb \pm yc$ é múltiplo de $a$.*

*Demonstração.* Existem números naturais $q$ e $t$ tais que $b = qa$ e $c = ta$. Portanto $xb \pm yc = xqa \pm yta = (xq \pm yt)a$, e vemos que $xb \pm yc$ é múltiplo de $a$. □

Dados números naturais $b$ e $c$, uma *combinação linear* de $b$ e $c$ é um número natural da forma $xb \pm yc$, sendo $x$ e $y$ números naturais. Tendo isso em vista podemos reescrever o enunciado da proposição acima da seguinte forma: se dois números naturais são múltiplos de um número natural $a$, então qualquer combinação linear desses números também é múltiplo de $a$. Ou então, se $a \neq 0$, podemos também enunciar: se $a$ divide $b$ e $c$ então $a$ divide qualquer combinação linear de $b$ e $c$.

No estudo dos números naturais através de sua decomposição multiplicativa, um dos primeiros fatos que nos chama a atenção é que podemos decompor os números em uma sequência de produtos até obter unicamente fatores primos. Exemplos de sequências de decomposição de alguns números:

$$\begin{aligned} 12 &= 4 \times 3 \\ &= 2 \times 2 \times 3 \end{aligned} \qquad \begin{aligned} 7007 &= 7 \times 1001 \\ &= 7 \times 7 \times 143 \\ &= 7 \times 7 \times 11 \times 13 \end{aligned} \qquad \begin{aligned} 30039 &= 3 \times 10013 \\ &= 3 \times 17 \times 589 \\ &= 3 \times 17 \times 19 \times 31 \end{aligned}$$

sendo 2, 3, 7, 11, 13, 17, 19, 31 números primos. Portanto encontramos, para cada um dos números 12, 7007 e 30039, uma decomposição com os menores fatores possíveis. Vemos assim que os números primos são os elementos mínimos da estrutura multiplicativa dos números naturais. Mais exatamente temos o

**Teorema 4.22.** *Todo número natural $\geq 2$ é primo ou se escreve como produto de primos.*

*Demonstração.* Seja $n \geq 2$ um número natural. Notemos que $n$ tem pelo menos um fator $> 1$, o próprio $n$. Seja $p_1$ o menor dos fatores $> 1$ de $n$. Então $p_1$ é primo porque, se não o fosse, $p_1$ teria um fator $q$ com $1 < q < p_1$, e $q$ seria também um fator $> 1$ de $n$, contrariando ser $p_1$ o menor deles. Ponhamos $n = p_1 n_1$, e notemos que $1 \leq n_1 < n$. Se $n_1 = 1$ então $n$ é primo e terminamos. Se $n_1 > 1$, decompomos $n_1$ de forma análoga, e escrevemos $n_1 = p_2 n_2$, com $p_2$ primo e $1 \leq n_2 < n_1$. Temos $n = p_1 p_2 n_2$. Se $n_2 = 1$, terminamos. Se $n_2 > 1$, repetimos o procedimento decompondo-o de forma análoga. Prosseguindo, obtemos números primos $p_1$, $p_2$, ..., $p_i$, ... e uma sequência decrescente de números naturais $n > n_1 > n_2 > \ldots > n_i > \ldots \geq 1$ tais que $n = p_1 p_2 \ldots p_i n_i$, continuando com a decomposição sempre que $n_i > 1$. Como de 1 a $n$ existe uma quantidade finita de números naturais, o procedimento acima tem um último passo no qual se obtém $n_k = 1$, e ficamos com um produto $n = p_1 p_2 p_3 \ldots p_k$, em que cada $p_i$ é primo. □

Uma consequência imediata mas importante é o

**Escólio 4.23.** *Todo número natural $\geq 2$ é múltiplo de (pelo menos) um número primo.*

Em outros termos, todo número natural $> 1$ tem fator primo (se o número é primo, esse fator é ele mesmo). A justificativa dessa afirmação está contida na demonstração do Teorema acima: o menor fator $> 1$ de qualquer número natural é sempre primo.

**Definição 4.24.** Seja $n$ um número natural composto. Denominamos *decomposição em fatores primos* de $n$ a um produto $n = p_1 p_2 p_3 \cdots p_s$ em que cada $p_i$ é um número primo. Esse produto também se diz *fatoração de $n$ em primos.*

É possível que alguns desses primos, ou mesmo todos, apareçam mais de uma vez na decomposição. Por exemplo, $36 = 2 \cdot 2 \cdot 3 \cdot 3$. Para condensar essa representação podemos escrever $36 = 2^2 \cdot 3^2$, o que sugere a

**Definição 4.25.** Seja $n$ um número natural composto. Denominamos *decomposição canônica em fatores primos* de $n$, ou simplesmente *decomposição canônica* de $n$, ou ainda *fatoração canônica* de $n$, a um produto $n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \cdots p_s^{\alpha_s}$ em que cada $p_i$ é um número primo, $p_i \neq p_j$ se $i \neq j$, e $\alpha_i \geq 1$.

Essas descobertas sobre os números naturais, feitas pela Escola Pitagórica, trouxeram importantes perguntas que determinaram o desenvolvimento posterior da Teoria dos Números. Algumas dessas perguntas são:

1. A quantidade de números primos é finita ou infinita?

2. Como testar a primaridade de um número? (testar a primaridade de um número significa verificar se o número é primo ou não.)

3. Como produzir uma lista dos números primos da forma mais rápida e cômoda possível?

4. Dado um número composto, como encontrar seus fatores primos?

5. A decomposição de um número natural $n \geq 2$ como produto de fatores primos é única (a menos da ordem dos fatores)?

6. A sequência dos números primos tem uma regra de formação que possa facilitar sua obtenção? Existe uma fórmula adequada que forneça o $n$-ésimo número primo?

Alguns desses problemas podem se tornar muito complicados se observarmos que necessitamos de um método que possa resolvê-los com recursos limitados. Por exemplo, se um método prevê gastar 100 anos para testar se um dado número (de bom tamanho) é ou não primo, então esse método pode não servir para muitos propósitos.

Vamos trabalhar com essas questões nos próximos capítulos, em que daremos continuidade aos nossos estudos sobre números primos e compostos. Nesse ponto advertimos o estudante interessado de que para prosseguir seus estudos em Teoria dos Números é necessário observar silenciosamente e atentamente os números, assim como o estudo da Astronomia exige a observação prolongada dos céus (confira [60], página xiv).

**Problema resolvido 4.26.** Se $a$ e $b$ são números naturais tais que $a$ é múltiplo de $b$ e $a < b$ então $a = 0$. De forma equivalente temos: se $a$ e $b$ são números naturais tais que $a$ é múltiplo de $b$ e $a > 0$ então $b \leq a$.

*Solução.* Como $a$ é múltiplo de $b$ existe um número natural $q$ tal que $a = bq$. Se fosse $q \geq 1$ teríamos $b \cdot q \geq b \cdot 1 \Rightarrow a \geq b$, o que é uma contradição com a hipótese de que $a < b$. Portanto $q = 0$ e segue que $a = 0$. Outra forma de escrever: se $a > 0$ é múltiplo de $b$ existe um número natural $q$ tal que $a = bq$. Não podemos ter $q = 0$, pois $a > 0$. Então $q \geq 1$. Multiplicando por $b$ ambos os lados dessa desigualdade vem $bq \geq b$, o que implica $a \geq b$. □

**Problema resolvido 4.27.** Demonstre que se $m > 1$ é um número natural que não é múltiplo de 3 então $m^2 + 2$ é composto.

*Solução.* Um número natural $m > 1$ que não é múltiplo de 3 é de uma das seguintes formas: $m = 3q+1$ para algum número natural $q > 0$, ou $m = 3q+2$ para algum número natural $q \geq 0$. Se $m = 3q + 1$ então $m^2 + 2 = (3q + 1)^2 + 2 = 9q^2 + 6q + 3 = 3(3q^2 + 2q + 1)$. Como $q > 0$ vemos que $3q^2 + 2q + 1 > 1$, e assim $m^2 + 2$ é produto de dois números naturais $> 1$. Portanto $m^2 + 2$ é composto (confira o Problema 4.10.3 abaixo). Por outro lado, se $m = 3q + 2$ então $m^2 + 2 = (3q + 2)^2 + 2 = 9q^2 + 12q + 6 = 3(3q^2 + 4q + 2)$, e $m^2 + 2$ novamente é produto de dois números naturais $> 1$, logo é composto. □

**Problema resolvido 4.28.** Demonstre que todo número natural da forma $3n + 2$ tem um fator primo também dessa forma.

*Solução.* Se $3n + 2$ for primo nada há a demonstrar. Se não for, o Teorema 4.22 garante que $3n + 2$ é um produto de primos. Nenhum desses primos é 3, pois 3 não é fator de $3n + 2$. Portanto, esses primos são da forma $3t + 1$ ou $3t + 2$. Se todos fossem da forma $3t + 1$, o resultado do Problema 4.10.16 proposto logo abaixo garante que seu produto também seria da mesma forma, mas não é. Logo pelo menos um dos primos que comparecem na decomposição de $3n + 2$ é dessa forma. □

**Problema resolvido 4.29.** Encontre todos os primos $p$ tais que $3p+1$ é um quadrado perfeito.

*1ª. solução.* Seja $3p + 1 = a^2$, sendo $a$ um número natural e $p$ um primo. Temos $3p = (a-1)(a+1)$, portanto $3p$ é produto dos números naturais $a-1$ e $a+1$. Mas $3p$ se escreve como um produto de dois números naturais das seguintes maneiras:
*1ª. maneira:* $(1)\cdot(3p)$ Temos $a-1=1$ e $a+1=3p$, o que não é possível, pois isso implica $a=2$ e $p=1$.
*2ª. maneira:* $(3p)\cdot(1)$ Temos $a-1=3p$ e $a+1=1$, o que implica $a=0$, o que não é possível.
*3ª. maneira:* $(3)\cdot(p)$ Temos $a-1=3$ e $a+1=p$, o que implica $a=4$ e $p=5$, que é uma solução possível.
*4ª. maneira:* $(p)\cdot(3)$ Temos $a-1=p$ e $a+1=3$, o que implica $a=2$ e $p=1$, o que novamente não é possível.

Resposta: $p=5$ é a única solução possível.

*2ª. solução.* Escrevendo $3p+1=a^2$, lembramos que $a$ está em uma das classes módulo três. Temos assim três casos a considerar:
*1º caso:* $a=3k$ para algum número natural $k$. Então $3p+1=9k^2$, o que não é possível, pois $9k^2$ é múltiplo de 3 mas $3p+1$ não é.
*2º caso:* $a=3k+1$ para algum número natural $k$. Então $3p+1=(3k+1)^2=9k^2+6k+1 \Rightarrow 3p=9k^2+6k \Rightarrow p=3k^2+2k=k(3k+2)$. Como $p$ é primo e $3k+2>1$ vem que $k=1 \Rightarrow p=5$, que é uma solução possível.
*3º caso:* $a=3k+2$ para algum número natural $k$. Então $3p+1=(3k+2)^2=9k^2+12k+4 \Rightarrow 3p=9k^2+12k+3 \Rightarrow p=3k^2+4k+1=(k+1)(3k+1)$. Como $p$ é primo segue $k+1=1$ ou $3k+1=1 \Rightarrow k=0 \Rightarrow a=2 \Rightarrow p=1$, o que não é possível.

Novamente a resposta é: $p=5$ é a única solução possível.

*3ª. solução.* Escrevendo $3p+1=a^2$, temos $3p=(a-1)(a+1)$. Observamos que os números $a-1$, $a$ e $a+1$ são consecutivos, e assim um deles é múltiplo de 3. Temos três possibilidades:
*1ª. possibilidade:* $a-1=3k$. Então $3p=3k(a+1) \Rightarrow p=k(a+1) \Rightarrow k=1$ ou $a+1=1 \Rightarrow a=4$ ou $a=0$. Se $a=4$ temos $p=5$, que é uma solução possível. $a=0$ não é possível
*2ª. possibilidade:* $a=3k$. Então $3p=(a-1)(a+1)=(3k-1)(3k+1)=9k^2-1$, o que não é possível, pois $3p$ é múltiplo de 3 mas $9k^2-1$ não é.
*3ª. possibilidade:* $a+1=3k$. Então $3p=(a-1)3k \Rightarrow p=(a-1)k \Rightarrow a-1=1$ ou $k=1 \Rightarrow a=2 \Rightarrow p=1$ o que não é possível.

Novamente a resposta é: $p=5$ é a única solução possível.

*4ª. solução.* Escrevendo $3p+1=a^2$, temos $3p=(a-1)(a+1)$. O Problema 4.8.23 garante que 3 divide $a-1$ ou $a+1$. Temos assim dois casos a considerar:
*1º caso:* $a-1=3k$. Já vimos que essa situação conduz a $p=5$.
*2º caso:* $a+1=3k$. Já vimos que essa situação não é possível.

Novamente a resposta é: $p=5$ é a única solução possível. □

## 4.10 Problemas

**Problema 4.10.1.** Explique por que 2 é o único primo par, e por que 3 é primo. E quanto a 5 e 7? Explique por que todo composto é $\geq 4$.

**Problema 4.10.2.** Explique por que é ímpar todo número natural que divide outro número ímpar.

**Problema 4.10.3.** O texto definiu número composto se for $> 1$ e se tiver algum fator $\neq 1$ e menor do que ele mesmo. Explique por que a seguinte definição é equivalente: $n$ é composto quando $n = pq$ com $p, q > 1$.

**Problema 4.10.4.** Explique por que, dado um número natural $n > 1$, seu conjunto de fatores $> 1$ é finito e não vazio.

**Problema 4.10.5.** Seja $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, ..., $p_i$,... a lista dos primos em ordem crescente. Explique por que todo número natural $n \geq 1$ se escreve na forma $n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \cdots p_i^{\alpha_i} \cdots$ com $\alpha_i \geq 0$, sendo que existe $k \geq 1$ tal que $\alpha_i = 0$ para todo $i \geq k$. Aqui se admite que o produto de infinitos 1's é 1.

**Problema 4.10.6.** Seja $n \geq 1$ um número natural. Explique por que $n$ pode ser escrito na forma $n = 2^s b$ para algum $s \geq 0$ e para algum ímpar $b$. Demonstre que essa decomposição é única, isto é, se também $n = 2^t c$ com $t \geq 0$ e $c$ ímpar, então $t = s$ e $c = b$.

*Solução.* Vejamos primeiro a existência da decomposição. Se $n$ for ímpar, pomos $n = 2^0 n$, como $s = 0$ e $b = n$. Se $n$ for par, a decomposição canônica $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ tem um primo igual a 2, digamos que seja $p_1$, renomeando os primos se necessário. Então os outros primos são ímpares, e seu produto é ímpar. Chamando esse produto de $b$ e pondo $\alpha_1 = s$, temos $n = 2^s b$.

Vejamos agora a unicidade. Temos $2^s b = 2^t c$. Se fosse $s > t$ teríamos $2^{s-t} b = c$, com $s - t > 0$, o que é uma contradição, pois $2^{s-t} b$ é par e $c$ é ímpar. Igualmente a condição $s < t$ também levaria a uma contradição. Logo $s = t$. Segue que $c = b$. □

**Problema 4.10.7.** Explicite em algumas palavras que método temos até o momento para verificar se um dado número é primo ou não. Isto é, testar a primaridade de um dado número. Que tipo de economia nos cálculos é possível fazer nesse método? Aplique esse método para ver que os números 11, 13, 17, 19, 503 e 809 citados no texto como primos o são efetivamente.

**Problema 4.10.8.** Demonstre que se $a$, $b$ e $c$ são números naturais tais que $c$ divide $a + b$ e $c$ divide $a$, então $c$ divide $b$.

**Problema 4.10.9.** Demonstre que se $a$, $b$ e $c \neq 0$ são números naturais tais que $ac$ é múltiplo de $bc$, então $a$ é múltiplo de $b$. A hipótese $c \neq 0$ é necessária?

**Problema 4.10.10.** Encontre o menor ímpar composto. Encontre o menor ímpar composto que é produto de três primos (diferentes).

**Problema 4.10.11.** Seja $d$ um algarismo decimal e seja $n = (dd \ldots d)_{dez}$ um número natural tal que $n \geq 11$. Prove que se $n$ for primo então $d = 1$. Mostre que essa situação efetivamente ocorre, isto é, existem números $n$ da forma acima, com $d = 1$, que são primos.

**Problema 4.10.12.** Demonstre que um número natural $p > 1$ é primo se e somente se não se escreve na forma $p = ab$, com $a > 1$ e $b > 1$ números naturais.

**Problema 4.10.13.** (i) Demonstre que se $p$ e $q$ são primos tais que $p = aq$ para algum número natural $a$, então $p = q$. (ii) Demonstre que se $p$ é primo e $p = ab$ para números naturais $a$ e $b$, então $p = a$ ou $p = b$.

**Problema 4.10.14.** Se um primo $p$ é da forma $3n + 1$ para algum número natural $n$, o que você pode afirmar sobre $n$? Justifique.

**Problema 4.10.15.** **a)** Demonstre que se $p$ é primo então $p$ não pode dividir ao mesmo tempo um número natural e seu sucessor. **b)** Demonstre que se $p$ é primo ímpar então $p$ não pode dividir ao mesmo tempo um número natural $n$ e seu sucessor de mesma paridade $n+2$.

**Problema 4.10.16.** Demonstre que o produto de dois ou mais números naturais da forma $3t+1$ ainda é dessa forma.

**Problema 4.10.17.** Demonstre as seguintes afirmações de Theon de Smyrna: **a)** Se $m$ é um número natural, então ou $m^2$ ou $m^2-1$ é múltiplo de 3. **b)** Se $m$ é um número natural, então ou $m^2$ ou $m^2-1$ é múltiplo de 4.

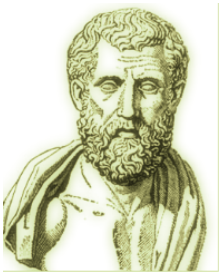
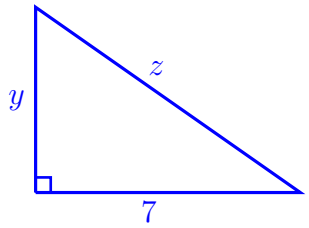


Figura 4.7. Desenho representando Theon de Smyrna, filósofo, matemático e astrônomo da Antiga Grécia. Pertenceu à Escola Pitagórica. Escreveu comentários para o entendimento da obra de Platão, em que abordou números pares e ímpares, primos, perfeitos e abundantes, além de um estudo sobre as melhores aproximações de $\sqrt{2}$ usando equações diofantinas.

**Problema 4.10.18.** Identifique todos os números primos da forma $(a_1a_0)_{dez}$ tais que $a_1 \times a_0$ também é primo.

**Problema 4.10.19.** Demonstre que se $n > 4$ é composto então $n$ é fator de $(n-1)!$

**Problema 4.10.20.** Um triângulo retângulo tem catetos 7 e $y$, e hipotenusa $z$. Sabendo que $y$ e $z$ são números naturais, calcule-os.




**Problema 4.10.21.** Verifique se o seguinte argumento pode ser usado para demonstrar que existem infinitos números primos. Existem infinitos números naturais, certo? Como os primos são os "blocos construtivos" dos naturais, então (?) há que existirem infinitos deles.

**Problema 4.10.22.** Demonstre os seguintes critérios de divisibilidade no sistema decimal. **a)** *critério de divisibilidade por 4:* um número natural $(a_na_{n-1}\ldots a_1a_0)_{dez}$ é múltiplo de 4 se e somente se $(a_1a_0)_{dez}$ o for. **b)** *critério de divisibilidade por 5:* um número natural $(a_na_{n-1}\ldots a_1a_0)_{dez}$ é múltiplo de 5 se e somente se $a_0 = 0$ ou $a_0 = 5$. **c)** *critério de divisibilidade por 10:* um número natural $(a_na_{n-1}\ldots a_1a_0)_{dez}$ é múltiplo de 10 se e somente se $a_0 = 0$.

**Problema 4.10.23.** O que se pode afirmar sobre a representação decimal de um número que é múltiplo de 50? Por quê?

**Problema 4.10.24.** Um estudante, perguntado se 458 941 é múltiplo de 7, fez os seguintes cálculos:

$$
\begin{array}{cccccc}
4 & 5 & 8 & 9 & 4 & 1 \\
 & & & - & 2 & 1 \\
\hline
4 & 5 & 8 & 9 & 2 & 0 \\
 & & - & 4 & 2 & \\
\hline
4 & 5 & 8 & 5 & 0 & \\
 & - & 3 & 5 & & \\
\hline
4 & 5 & 5 & 0 & & \\
- & 3 & 5 & & & \\
\hline
4 & 2 & 0 & & &
\end{array}
$$

Como 42 é múltiplo de 7, então 458 941 também é, concluiu o estudante.
**a)** Verifique se o estudante está correto e explique seu raciocínio. **b)** Comprove se o método do estudante possibilita verificar a multiplicidade por 7 de qualquer número natural escrito no sistema decimal. **c)** Investigue para quais números, além de 7, o método funciona.

**Problema 4.10.25.** Demonstre o seguinte critério de divisibilidade por seis: um número natural é múltiplo de 6 se e somente se for múltiplo de 2 e de 3. Alguma generalização?

**Problema resolvido 4.30.** Se $p$ e $p+2$ são primos os denominamos *primos gêmeos*. O estudante pode examinar a lista de primos do Apêndice A, e ver que existem muitos primos gêmeos. Investigue se existem muitos primos *trigêmeos*, isto é, $p$, $p+2$ e $p+4$ que sejam todos primos. Um exemplo é 3, 5 e 7.

*1ª. solução.* Já sabemos que se $p = 3$ então $p$, $p+2$ e $p+4$ são primos trigêmeos. Suponhamos $p > 3$. O Problema 4.8.20 pede para provar que para todo número natural $n$ exatamente um dos números $n$, $n+2$ ou $n+4$ é múltiplo de 3. Portanto $p$, $p+2$ e $p+4$ não podem ser todos primos, a não ser que $p = 3$.

*2ª. solução.* Vamos examinar alguns ternos de números $p$, $p+2$ e $p+4$, com $p$ primo, e tentar perceber alguma regularidade. Temos:

| $p$ | $p+2$ | $p+4$ |
|---|---|---|
| 5 | 7 | 9 |
| 7 | 9 | 11 |
| 11 | 13 | 15 |
| 13 | 15 | 17 |
| 17 | 19 | 21 |

Observamos que em cada linha existe um múltiplo de 3 e ele está às vezes na segunda coluna, outras vezes na terceira. Examinando mais de perto vemos que se $p = 3q+1$ para algum natural $q$ então o múltiplo de 3 está na segunda coluna, e se $p = 3q+2$ para algum natural $q$ então o múltiplo de 3 está na terceira coluna. Agora é fácil obter uma prova geral. Se $p = 3q+1$ então $p+2 = 3q+1+2 = 3q+3 = 3(q+1)$. Se $p = 3q+2$ então $p+4 = 3q+2+4 = 3q+6 = 3(q+2)$. Esses múltiplos de 3 são sempre $> 3$ portanto nunca são primos. Como todo primo $p > 3$ é da forma $p = 3q+1$ ou $p = 3q+2$ para algum natural $q$, fica provado que não existem primos trigêmeos $p$, $p+2$ e $p+4$, com $p > 3$. □

**Problema resolvido 4.31.** Considere a sequência 1, 2, 2, 3, 3, 3, 4, 4, 4, 4, 5, 5, 5, 5, 5, 6, ... formada pelos números naturais em ordem crescente, sendo que o número $n$ aparece $n$ vezes consecutivas. Calcule o 2010º termo.

*Solução.* Ao escrever a sequência desde o início temos: escrevendo o número 1 escrevemos 1 número no total; terminando de escrever o número 2 escrevemos $1+2$ números no total; terminando de escrever o número 3 escrevemos $1+2+3$ números no total; e, assim por diante, terminando de escrever o número $k$ escrevemos $1+2+3+\ldots+k$ números no total.

Como $1+2+3+\ldots+k = k(k+1)/2$, calculamos $k$ tal que $k(k+1)/2 = 2010$, e encontramos $k \approx -63,9$ e $k \approx 62,9$. Rejeitamos o valor negativo e arredondamos para baixo o segundo (esse valor não é um número natural certamente porque o 2010º termo não é o último da lista do mesmo número). Calculamos $62(62+1)/2 = 1953$, o que significa que ao terminarmos de escrever 62 vezes o número 62 atingimos o 1953º termo da sequência. Os próximos 63 termos da sequência são todos constituídos pelo número 63. Como $1953+63 = 2016$, segue que o 2010º termo da sequência é 63. □

## 4.11 Teoria aditiva dos números naturais

Estivemos estudando os números naturais mediante sua decomposição como produto de outros números. Para isso usamos muito a multiplicação e a divisão. Alternativamente podemos estudar propriedades dos números naturais considerando sua partição como soma de números de um determinado tipo. É o que se chama de *teoria aditiva*.

Como exemplo lembramos que já sabemos que todo número natural positivo se escreve como soma de diferentes potências de 2, e de uma única forma, desconsiderando-se a ordem das parcelas. Assim para decompor 37 calculamos sua representação binária:

$$37 = (100101)_{dois} = 1\cdot 2^5 + 0\cdot 2^4 + 0\cdot 2^3 + 1\cdot 2^2 + 0\cdot 2^1 + 1\cdot 2^0,$$

de modo que

$$37 = 2^5 + 2^2 + 2^0.$$

Como a representação binária é única, essa é a única representação de 37 como soma de potências de 2, a menos da ordem das parcelas. Para mais detalhes confira o Problema 2.12.15.

Por *partição* de um número natural positivo se entende sua representação como soma de números naturais positivos (pode ser "soma" de uma só parcela). Nesse tipo de representação não são distinguidas duas representações que diferem apenas pela ordem de parcelas. Vejamos alguns exemplos:

$1 = 1$;

$2 = 1+1$;

$3 = 2+1 = 1+1+1$;

$4 = 3+1 = 2+2 = 2+1+1 = 1+1+1+1$;

$5 = 4+1 = 3+2 = 3+1+1 = 2+2+1 = 2+1+1+1 = 1+1+1+1+1$;

$6 = 5+1 = 4+2 = 4+1+1 = 3+3 = 3+2+1 = 3+1+1+1 = 2+2+2 =$
$= 2+2+1+1 = 2+1+1+1+1 = 1+1+1+1+1+1.$

Indicando por $p(n)$ a quantidade de partições de $n$, vemos que $p(1) = 1$, $p(2) = 2$, $p(3) = 3$, $p(4) = 5$, $p(5) = 7$ e $p(6) = 11$. Fazendo mais experimentos numéricos, a primeira constatação é que $p(n)$ aumenta muito rapidamente. Por exemplo,

$$p(10) = 42, \quad p(20) = 627, \quad p(30) = 5604, \quad p(100) = 190\,569\,292.$$

São conhecidas fórmulas recorrentes e assintóticas para $p(n)$. Uma das mais simples foi descoberta por Srinivasa I. Ramanujan. Para mais detalhes consulte [108], a partir da página 160, assim como [125], no item *Partition Function P.*



Figura 4.8. Foto de Srinivasa Ramanujan Aiyangar, genial matemático hindu. Foi um autodidata, e usava um método próprio para estudar Matemática. Contribuiu em Teoria dos Números, Análise, séries infinitas e frações contínuas. Durante sua curta vida desenvolveu aproximadamente 3 900 identidades e equações. Ramanujan, em geral, não fornecia demonstrações de seus resultados, e, ao que parece, ele mesmo não as tinha. Mas a maioria delas foi posteriormente confirmada e demonstrada por outros matemáticos.

Podemos considerar também decomposições de números naturais como soma e diferença de números de um dado conjunto. Vemos no Problema 6.6.13, que, usando a representação ternária balanceada, podemos escrever qualquer número natural de forma única como soma e diferença de diferentes potências de 3. Por exemplo,

$$148 = 3^5 - 3^4 - 3^3 + 3^2 + 3^1 + 3^0$$

O estudante está convidado a investigar outros resultados sobre a abordagem aditiva no Problema 4.12.22 e nos temas 4.14.9, 4.14.10 e 4.14.11.

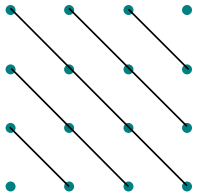
## 4.12 Problemas adicionais

**Problema 4.12.1.** Um professor, ao aplicar atividades de resolução de problemas em suas aulas, prefere repartir os estudantes em grupos de três. Explique por que $n \geq 2$ estudantes podem sempre serem repartidos em grupos de três e no máximo dois grupos de dois.

**Problema 4.12.2.** Verifique que, dados dois números naturais pares consecutivos, exatamente um deles é múltiplo de 4.

**Problema 4.12.3.** Determine condições necessárias e suficientes sobre os números naturais $m$ e $n$ para que a potência $m^n$ seja **a)** par; **b)** ímpar.

**Problema 4.12.4.** Dado o número figurado $4^2$, consideremos linhas paralelas à diagonal principal, conforme a figura abaixo.



Isso nos sugere $1+2+3+4+3+2+1 = 4^2$. Generalize. Use essa observação para verificar a fórmula $1+2+3+\cdots+n = (1/2)n(n+1)$. Você fez uma indução ou uma dedução?

**Problema 4.12.5.** Prove que todo número pentagonal $P_n$ com $n \geq 1$ se escreve como a soma de um número quadrado com um número triangular. Para completar o caso $n = 1$ defina o número triangular $T_0 = 0$.

**Problema 4.12.6.** O matemático hindu Aryabhata descobriu, por volta do ano 500, uma fórmula para a soma $T_1 + T_2 + T_3 + \cdots + T_n$ para todo número natural $n$. Faça isso você também.



Figura 4.9. Foto de estátua de Aryabhata, matemático e astrônomo da idade clássica da Índia. Em seu tratado sobre Matemática abordou Aritmética, Álgebra, trigonometria plana e esférica, frações contínuas, equações quadráticas, séries de potências e apresentou uma tábua para o seno.

**Problema 4.12.7.** Tomando os números naturais positivos em ordem consideramos conjuntos formados por eles, o primeiro com o número 1, o segundo com os dois seguintes, o terceiro com os três subsequentes, etc. Temos assim

$$\{1\} \quad \{2,3\} \quad \{4,5,6\} \quad \{7,8,9,10\} \quad \ldots$$

Em que conjunto aparece o número 2000? Dê o primeiro número do conjunto, o último e a ordem na qual 2000 aparece no conjunto.

**Problema 4.12.8.** Os números naturais de 1 a 2010 são escritos em um grande quadro negro. Em seguida, um estudante apaga dois quaisquer desses números e escreve no quadro sua diferença (positiva ou zero). Repete a operação até que um único número fique escrito no quadro. É possível que esse número seja zero?

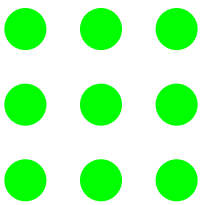
**Problema 4.12.9.** Em um plano existem 11 cidades numeradas de 1 a 11. Estradas retilíneas ligam 1 a 2, 2 a 3, 3 a 4, 4 a 5, 5 a 6, 6 a 7, 7 a 8, 8 a 9, 9 a 10, 10 a 11, e 11 a 1. Se as cidades estiverem em uma posição favorável, é possível construir uma estrada retilínea adicional cortando todas essas estradas e que não passe por nenhuma cidade?

**Problema 4.12.10. a)** Consideremos os números naturais de 1 a 10, escritos em fila:

$$1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \quad 7 \quad 8 \quad 9 \quad 10$$

**a)** Antes de cada um deles coloque sinais "+" ou "−" de forma que o cálculo da expressão resulte zero. **b)** Resolva problema similar para os números de 1 a 11.

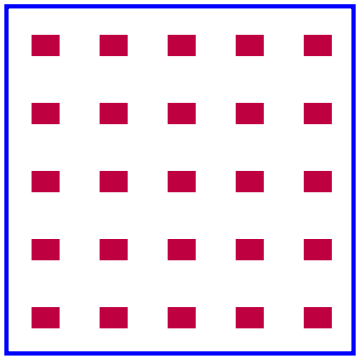
**Problema 4.12.11.** Resolva o problema abaixo e considere outros problemas similares obtidos mediante sua modificação.



Um jogo tem 9 botões luminosos dispostos como na figura. Cada botão pode ficar de cor verde ou vermelha. Apertando um botão do bordo do retângulo, trocam de cor ele e seus vizinhos (vizinhos na direção horizontal, vertical ou diagonal). Apertando o botão do centro, trocam de cor todos os seus 8 vizinhos porém ele não. Inicialmente todos os botões estão verdes. É possível, apertando sucessivamente alguns botões, torná-los todos vermelhos?

**Problema 4.12.12.** Uma classe tem 25 carteiras, e cada carteira está ocupada por um estudante. Entra o professor de Matemática, e diz: — Todo aluno desta classe deve, uma única vez, trocar de carteira com um colega. Pergunta-se: será possível cumprir o pedido do professor?

**Problema 4.12.13.** Resolva o problema abaixo e considere também modificações, tomando classes no formato $n \times m$.
Uma classe tem 25 carteiras dispostas de acordo com a figura. Cada carteira está ocupada por um estudante. Entra o professor de Matemática, e diz: — Todo aluno desta classe deve mudar de carteira, uma única vez, passando para uma carteira contígua à sua, na direção horizontal ou vertical. Pergunta-se: será possível cumprir o pedido do professor?



**Problema 4.12.14.** Em uma festa comparecem 9 pessoas. Algumas se cumprimentam com um aperto de mão, outras não. Confira se é possível que cada pessoa cumprimente exatamente outras 3.

**Problema 4.12.15.** Em um plano munido de um sistema de coordenadas cartesianas $Oxy$ considere a reta $x - y + 17 = 0$. Quantos e quais são os pontos $(p, q)$ do plano pertencentes à reta com $p$ e $q$ primos?

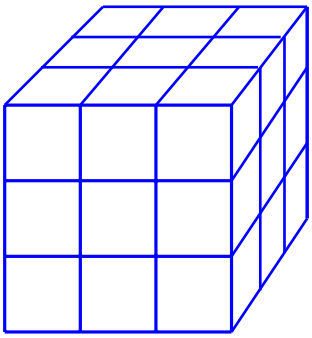
**Problema 4.12.16.** Em um plano munido de um sistema de coordenadas cartesianas $Oxy$ considere a circunferência $x^2 + y^2 = 7373$. Justifique por que nessa circunferência existem pontos $(x, y)$ sendo $x$ e $y$ números naturais. Quantos e quais são os pontos $(p, q)$ do plano pertencentes à circunferência com $p$ e $q$ primos?

**Problema 4.12.17.** Verifique se os números naturais $a$, $b$ e $\log_b a$ podem ser todos primos.

**Problema 4.12.18.** Demonstre o seguinte resultado atribuído à Escola Pitagórica: se um ímpar divide um par, então o ímpar também divide a metade do par.

**Problema 4.12.19.** Pegue uma folha de papel e corte-a em cinco pedaços. Pegue um dos pedaços e corte-o em cinco pedaços. Após ter feito isso várias vezes é possível obter exatamente 1000 pedaços de papel? e 1001?

**Problema 4.12.20.** Um cubo de lado 3 é subdividido em 27 cubos unitários. Escolhemos um dos cubos unitários posicionado no centro de uma das faces, e o denominamos $A$. Do centro do cubo unitário $A$ traçamos um segmento até o centro de um cubo adjacente qualquer $B$, que tem uma face comum com $A$. Do centro do cubo unitário $B$ traçamos um segmento até o centro de um cubo adjacente qualquer $C$, que tem uma face comum com $B$. E assim por diante, pergunta-se se é possível traçar uma linha poligonal passando uma única vez pelos centros de todos os cubos unitários, iniciando no centro do cubo $A$ e com ponto final no centro do cubo maior.



**Problema 4.12.21.** Prove que 4 não é fator de $n^2 + 2$ para todo número natural $n$.

**Problema 4.12.22.** Demonstre que a chamada "conjectura forte" de Christian Goldbach
**A)** *Todo número natural par* $> 2$ *é soma de dois primos (não necessariamente diferentes).*
é equivalente à seguinte afirmação:
**B)** *Todo número natural* $> 5$ *é soma de três primos (não necessariamente diferentes)*



Figura 4.10. Christian Goldbach foi um matemático nascido em Königsberg, antiga Prússia. A partir de 1725 foi professor da recém-fundada Academia de Ciências de São Petersburgo, Rússia, tendo exercido posteriormente o cargo de Ministro das Relações Exteriores daquele país. Conheceu e se correspondia com grandes matemáticos de sua época, e manteve uma constante amizade e correspondência com Leonhard Euler. Goldbach fez várias descobertas em Teoria dos Números, mas é mais conhecido por sua conjectura, ainda em aberto: *todo número natural* $> 2$ *é a soma de dois números primos.* Ao lado, página de carta de 1742 de Christian Goldbach a Leonhard Euler.

Consulte os verbetes da Wikipedia *Christian Goldbach* e *Goldbach's conjecture* para saber mais sobre Christian Goldbach e sua famosa conjectura.

## 4.13 Pequeno exemplo de investigação

Um problema com presença quase certa em qualquer livro didático de Teoria dos Números:

*com quantos zeros termina* 136! *?*

ou, mais geralmente: *com quantos zeros termina* $n$! *?*

Lembramos que para todo número natural $n \geq 1$ o número $n!$ chama-se *fatorial* de $n$, e consiste do produto de todos os números naturais $\geq 1$ até $n$, inclusive. Ou seja,

$$n! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdots (n-1) \cdot n$$

Se $n = 1$ isso significa $1! = 1$. Podemos estender essa definição estabelecendo que $0! = 1$. Escolhemos esse valor para 0! por conveniência, pois combina com muitas fórmulas.

Uma ideia inicial para resolver o primeiro problema seria calcular 136! Mas se trata de um número muito grande, é preciso usar um aplicativo computacional especial. De toda forma, não queremos examinar apenas o número 136! mas qualquer $n!$ Para isso necessitamos perceber nesses produtos alguma propriedade, algum comportamento repetitivo ou, como se diz, alguma regularidade.

Para um melhor entendimento da questão iniciamos examinando os primeiros produtos:

$0! = 1$;
$1! = 1$;
$2! = 1 \cdot 2 = 2$;
$3! = 1 \cdot 2 \cdot 3 = 6$;
$4! = 1 \cdot 2 \cdot 3 \cdot 4 = 24$;
$5! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 120$.

Vemos que o primeiro zero só apareceu para 5! o que nos lembra que 5 vezes um par resulta um número terminado em zero, e este, por sua vez, multiplicado por outros fatores resulta um produto final terminado em zero. Nenhum zero adicional aparece em 6! ou em 7! ou em 8! e nem em 9! todos eles terminam em um único zero.

Quando chegamos em 10! temos mais um motivo para aparecer outro zero, pois 10 como fator implica um zero no final da representação. Portanto

$$10! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 = 3\,628\,800$$

termina em dois zeros, assim como todos os fatoriais até 15!, quando aparece mais um zero. Desse a 19! todos terminam com três zeros.

Em seguida passamos para $n = 20$ e vemos que

$$\begin{aligned} 20! = {} & 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \cdot \text{ dois zeros} \\ & \cdot 11 \cdot 12 \cdot 13 \cdot 14 \cdot 15 \cdot 16 \cdot 17 \cdot 18 \cdot 19 \cdot 20 \text{ mais dois zeros,} \end{aligned}$$

portanto 20! termina com quatro zeros. Está inseguro? Podemos conferir com um aplicativo computacional:

$$20! = 2\,432\,902\,008\,176\,640\,000.$$

Percebemos assim uma regularidade: cada dezena tem dois múltiplos de 5, e cada um fornece um zero, a saber, um número terminado em 5, que multiplicado por um par fornece um zero, e um número teminado em zero, múltiplo de 10, que fornece outro zero.

Aparentemente temos a seguinte regra: para saber com quantos zeros termina $n!$, contamos quantas dezenas completas existem, e cada uma tem dois múltiplos de 5. Depois se vê a dezena não completa, se existir. Por exemplo, 136 tem 13 dezenas completas, o que fornece 26 zeros, e de 131 a 136 existe mais um múltiplo que 5, que é 135, e assim temos mais um zero. Será que 136! termina com 27 zeros?

Devagar ... é prudente pensar mais, examinar mais exemplos. Talvez nos escapou alguma coisa. Vejamos:

$$\begin{aligned} 30! = {} & 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 && \to \text{dois zeros no final da representação;} \\ & \cdot 11 \cdot 12 \cdot 13 \cdot 14 \cdot 15 \cdot 16 \cdot 17 \cdot 18 \cdot 19 \cdot 20 && \to \text{mais dois zeros;} \\ & \cdot 21 \cdot 22 \cdot 23 \cdot 24 \cdot 25 \cdot 26 \cdot 27 \cdot 28 \cdot 29 \cdot 30 && \to \text{hum ... 25 tem dois fatores 5.} \end{aligned}$$

Notemos que 25 multiplicado por dois pares ou por um múltiplo de 4 fornece mais dois zeros. Assim a terceira dezena de 30! fornece três zeros, de modo que esse número termina com

7 zeros.

Vemos que as dezenas não são todas iguais no que se refere à presença de um fator múltiplo de 5, pois 25 e seus múltiplos fornecem um zero adicional: 25, 50, 75, 100, 125, ... Bem, $125 = 5^3$ tem três fatores 5, de modo que 125 e seus múltiplos fornecem um terceiro zero adicional. E assim por diante.

Estamos agora diante de uma regra: a quantidade de zeros no final de $n!$ é:

$$\begin{aligned} &\textit{quantidade de múltiplos de 5 de 1 a } n \\ &+ \textit{ quantidade de múltiplos de } 25 = 5^2 \textit{ de 1 a } n \\ &+ \textit{ quantidade de múltiplos de } 125 = 5^3 \textit{ de 1 a } n \\ &+ \ldots \end{aligned}$$

Observe que essa soma é finita, pois paramos quando chegamos a uma potência de 5 maior do que $n$.

Vamos agora responder à pergunta inicial: *com quantos zeros termina* 136!*?* Como $136 \div 5 = 27$ com resto 1, $136 \div 25 = 5$ com resto 11 e $136 \div 125 = 1$ com resto 11, vemos que de 1 a 136, existem 27 múltiplos de 5, mais 5 múltiplos de 25 e mais 1 múltiplo de 125. Portanto a resposta é:

$$136! \text{ termina com } 27 + 5 + 1 = 33 \text{ zeros.}$$

Para encerrar nossa investigação, observamos que um estudante se preocupou com a seguinte questão: para que um fator 5 forneça um zero, ele precisa ser multiplicado por um número par. Existem pares suficientes? Por exemplo, se $n$ for maior do que $5^{35}$, esse número multiplicado por 35 pares fornece 35 zeros. E até chegar nesse número já foram usados muitos pares. Os pares são suficientes? Fica essa tarefa para o estudante desvendar. Uma ideia talvez possa ser encontrada no Tema 4.14.12, logo abaixo.

## 4.14 Temas para investigação

**Tema 4.14.1.** De acordo com o Problema 4.8.14 podemos observar que o critério de divisibilidade por 2 enunciado na Proposição 4.13 não se aplica para o sistema ternário. Descubra um critério de divisibilidade por 2 para o sistema ternário. E quanto a outros sistemas de numeração?

**Tema 4.14.2. a)** Divida por 8 os números $3^2$, $5^2$, $7^2$ e $9^2$. Que regularidades você observa? Faça mais alguns testes para constatar se as regularidades permanecem com outros valores. **b)** Transforme as regularidades em conjecturas gerais. Use algum método considerado válido pela Matemática para verificar se as conjecturas são verdadeiras ou falsas. Investigue as recíprocas de suas conjecturas. **c)** Que regularidades e conjecturas similares podem ser obtidas da sequência $2^2$, $4^2$, $6^2$,...?

**Tema 4.14.3.** O estudante deve ter resolvido o Problema 4.8.18:

*Determine o dígito da unidade do número* $N = 1 \cdot 3 \cdot 5 \cdot 7 \cdots 2007$*, produto dos ímpares de 1 a 2007.*

Certamente obteve a resposta correta de que o dígito é 5, e deve ter justificado. Explore mais esse problema, considerando mudanças de hipóteses. Isto é, invente problemas que tenham a mesma ideia mas com alguma modificação importante.

Por exemplo:

*Determine o dígito da unidade do número* $M = 1 \cdot 3 \cdot 7 \cdot 9 \cdot 11 \cdot 13 \cdot 17 \cdots 2007$*, produto dos ímpares de 1 a 2007 exceto aqueles que terminam em 5.*

**Tema 4.14.4.** Os números naturais de 1 a $n$ são escritos em um grande quadro negro. Em seguida, um estudante apaga dois quaisquer desses números e escreve no quadro sua diferença (positiva ou zero). Repete a operação até que um único número fique escrito no quadro. Para quais $n$ é possível que esse número seja zero?

**Tema 4.14.5.** Dado um número natural $n$ consideremos os números naturais de 1 a $n$ escritos em fila:

$$1 \quad 2 \quad 3 \quad 4 \quad 5 \quad \ldots \quad n$$

Caracterize os valores de $n$ para os quais é possível colocar antes de cada um dos números de 1 a $n$ sinais "+" ou "−" de forma que o cálculo da expressão resulte zero.

**Tema 4.14.6. a)** Uma jarra contém bolas vermelhas e bolas amarelas. Fora da jarra estão à disposição uma quantidade suficiente de bolas de ambas as cores. O seguinte procedimento é executado sempre que a quantidade de bolas na jarra for $\geq 2$: são retiradas duas bolas da jarra; se as duas tiverem a mesma cor, é colocada uma bola vermelha na jarra; se as duas tiverem cores diferentes, é colocada uma bola amarela na jarra. No final dessa brincadeira quantas bolas amarelas restam, e quantas vermelhas? **b)** Invente um problema similar envolvendo bolas de três cores.

**Tema 4.14.7. a)** Um estudante calculou o valor dos primeiros números cúbicos $0^3$, $1^3$, $2^3$, $3^3$, ... e tirou os noves fora de cada um. Observou que ocorria uma certa regularidade. Encontre essa regularidade e justifique. **b)** Observando que

$$\underbrace{1}_{1^3} \quad \underbrace{3 \;\; 5}_{2^3} \quad \underbrace{7 \;\; 9 \;\; 11}_{3^3}$$

descubra você também um teorema de Nicômaco de Gerasa. **c)** Um certo subconjunto infinito de números naturais são dispostos em linhas, em um arranjo cujas quatro primeiras linhas estão escritas a seguir. Encontre regularidades nesse arranjo. Demonstrações?

$$\begin{array}{cccc} 1 & & & \\ 3 & 5 & & \\ 6 & 9 & 12 & \\ 10 & 14 & 18 & 22 \\ \vdots & & & \end{array}$$

**d)** Investigue outras propriedades dos números cúbicos. Investigue também se as propriedades estudadas aqui para números cúbicos se estendem para outras potências, como as quadradas, as quárticas, as quínticas, etc.

**Tema 4.14.8.** Se $p$ e $p+2$ são primos, eles são chamados *primos gêmeos*, conforme vimos no Problema Resolvido 4.30. **a)** Faça uma lista de primos gêmeos. **b)** Descubra alguma propriedade interessante dos primos gêmeos. Sua propriedade pode facilitar a busca de primos gêmeos? **c)** Pesquise na literatura propriedades dos primos gêmeos. **d)** E quanto a triplos de primos? Quem sabe $p$, $p+2$ e $p+6$? Quádruplos?

**Tema 4.14.9.** Investigue que números naturais podem ser escritos como diferença de dois quadrados. Nos casos afirmativos desvende como calcular a quantidade de representações diferentes.

**Tema 4.14.10.** Podemos estender a definição de número triangular para $n = 0$ pondo $T_0 = 0$. Essa definição combina com as várias fórmulas elaboradas para $T_n$, como 4.1, 4.2 ou 4.3 dadas na página 100. J. C. F. Gauss provou em [44] que todo número natural pode ser escrito como uma soma de três números triangulares $T_n$, $n = 0, 1, 2, \ldots$ (não necessariamente diferentes). Verifique essa afirmação para todo número natural $\leq 50$. Alguma conjectura similar para números pentagonais?



Figura 4.11. Foto de pintura de Johann Carl Friedrich Gauss, importante matemático alemão que contribuiu nas áreas de Teoria dos Números, Álgebra, Estatística, Análise, Geometria Diferencial, Geofísica, Mecânica, Eletrostática, Astronomia, Ótica, dentre outras. Teve grande influência no desenvolvimento da Matemática e de outras ciências. Considerado um prodígio, sua maior obra, *Disquisitiones Arithmetica* [44], foi terminada quando tinha 21 anos, em 1798.

**Tema 4.14.11.** Investigue, começando com exemplos, resultados sobre a representação de números naturais como soma de quadrados. Faça conjecturas gerais. **a)** Examinando os números naturais $\leq 50$, veja que todos eles podem ser escritos como soma de no máximo quatro quadrados não nulos, não necessariamente diferentes. **b)** Que tipo de primos parece que podem ser escritos como soma de dois quadrados não nulos? Por exclusão, quais não podem? **c)** E quanto à soma de três quadrados?

**Tema 4.14.12.** Seja $n = 5^k$, com $k \geq 1$. Escreva $n! = 2^t 5^s q$, sendo $2 \nmid q$ e $5 \nmid q$ (isto é, 2 não divide $q$ e 5 não divide $q$). (a) Calcule $s$. (b) Mostre que $t > s$. (c) Com quantos zeros termina a representação decimal de $n!$ ?

**Tema 4.14.13.** Um número natural se diz *polido* se puder ser escrito como a soma de dois ou mais números naturais consecutivos. Caso contrário, o número se diz *não-polido*. Descubra pelo menos uma regularidade sobre esses números. Alguma demonstração?

## 4.15 Sugestões de atividades orientadas

**Atividade 4.15.1.** Às vezes se diz que a Teoria dos Números estuda as propriedades *intrínsecas* dos números, isto é, aquelas propriedades que não dependem do particular sistema de numeração que está sendo usado para representar os números. O contrário é denominado propriedade *extrínseca*. Percorrendo o texto procure exemplos de propriedades intrínsecas e propriedades extrínsecas.

**Atividade 4.15.2.** O estudo da relação de pessoas autistas com números tem revelado aspectos interessantes sobre a capacidade do homem de reconhecer os números. Faça uma pesquisa sobre esse assunto.

**Atividade 4.15.3.** Assista documentários ou filmes sobre a vida de matemáticos importantes para a Aritmética e a Teoria dos Números. Johann Carl Friedrich Gauss e Srinivasa Ramanujan são duas boas escolhas.

**Atividade 4.15.4.** Informe-se sobre o desenvolvimento da Aritmética e da Teoria dos Números em livros de História da Matemática.

**Atividade 4.15.5.** Assinale em um mapa os principais locais relacionados com o desenvolvimento da Aritmética e da Teoria dos Números, como centros de estudo e locais de nascimento e vida de matemáticos.

# Capítulo 5

# Números primos e compostos

## 5.1 Introdução

Dado um número natural, como encontrar seus divisores?

Como determinar se um dado número natural é primo ou não?

Como fazer uma lista de números primos?

Existe uma infinidade de números primos?

O que são o *mdc* e o *mmc*?

Neste capítulo prosseguimos nossa análise dos números naturais mediante a investigação das propriedades dos números primos e compostos. Estudamos alguns dos problemas anteriormente colocados sobre números primos e compostos, como a infinitude dos primos, e apresentamos as propriedades mais elementares do máximo divisor comum e do mínimo múltiplo comum. São conceitos básicos mas muito importantes na Teoria dos Números.

## 5.2 Propriedades dos divisores de um número natural

Dado um número natural $n$, para encontrar seus divisores podemos fazer o trabalho braçal de dividi-lo por todos os números entre 1 e $n$. Sempre que a divisão der exata, encontramos um divisor. Certamente que podemos economizar muito esforço se compreendermos as propriedades gerais dos divisores. Isso é o que vamos fazer agora.

Indicamos por $\mathcal{D}(n)$ o conjunto dos divisores do número natural $n$. Nada melhor do que começar com alguns exemplos:

$$\begin{array}{ll}
\mathcal{D}(0) = \{1, 2, 3, 4, \ldots\} & \mathcal{D}(1) = \{1\} \\
\mathcal{D}(2) = \{1, 2\} & \mathcal{D}(3) = \{1, 3\} \\
\mathcal{D}(4) = \{1, 2, 4\} & \mathcal{D}(5) = \{1, 5\} \\
\mathcal{D}(6) = \{1, 2, 3, 6\} & \mathcal{D}(7) = \{1, 7\} \\
\mathcal{D}(8) = \{1, 2, 4, 8\} & \mathcal{D}(9) = \{1, 3, 9\} \\
\mathcal{D}(10) = \{1, 2, 5, 10\} & \mathcal{D}(11) = \{1, 11\} \\
\mathcal{D}(12) = \{1, 2, 3, 4, 6, 12\} & \mathcal{D}(15) = \{1, 3, 5, 15\}
\end{array}$$

O estudante poderá estender essa lista achando outros conjuntos de divisores, como $\mathcal{D}(16)$, $\mathcal{D}(25)$, $\mathcal{D}(30)$, $\mathcal{D}(60)$, etc.

Em certa ocasião estava trabalhando com estudantes de uma classe de um curso de Matemática, e lhes pedi que observassem regularidades relacionadas com esses conjuntos. Eles perceberam várias propriedades. Listamos algumas delas a seguir, e apresentamos outras na seção de problemas 5.3.

*Propriedade 1.* 1 e $n$ estão sempre em $\mathcal{D}(n)$ para todo número natural $n \neq 0$.

De fato, para todo número natural $n > 0$ se tem $n = 1 \cdot n$, portanto 1 e $n$ são sempre divisores de $n$. Observamos que para $n = 0$ também se tem $0 = 1 \cdot 0$, portanto 1 é divisor de 0, mas, por definição, admitimos que 0 não é divisor de número algum. Por isso excluímos $n = 0$ dessa propriedade.

*Propriedade 2.* Se $n \neq 0$ e se $m \in \mathcal{D}(n)$ então $m \leq n$.

De fato, se $m \in \mathcal{D}(n)$ e $n \geq 1$ então existe um número natural $s \geq 1$ tal que $n = sm$. Assim $m = 1 \cdot m \leq sm = n \Rightarrow m \leq n$.

*Propriedade 3.* Se $n \neq 0$ e se $m \in \mathcal{D}(n)$ então $m \leq n/2$ ou $m = n$. Em outros termos, entre $n/2$ e $n$ não existem divisores de $n$.

De fato, se $m \in \mathcal{D}(n)$ então existe $q$ tal que $n = mq$. Se $m < n$ não pode ser $q = 1$, assim $2 \leq q$. Segue que $2m \leq mq = n$ e então $m \leq n/2$. Portanto, $m = n$ ou $m \leq n/2$.

*Propriedade 4.* Se $n \neq 0$ e se $m \in \mathcal{D}(n)$ então o quociente da divisão de $n$ por $m$ também está em $\mathcal{D}(n)$.

De fato, se $m \in \mathcal{D}(n)$, o quociente $q$ da divisão de $n$ por $m$ satisfaz $n = mq$. Mas $n = mq$ significa também que $q$ é divisor de $n$.

*Propriedade 5.* Se $m \in \mathcal{D}(n)$ então $\mathcal{D}(m) \subset \mathcal{D}(n)$.

Fica para o estudante demonstrar essa propriedade.

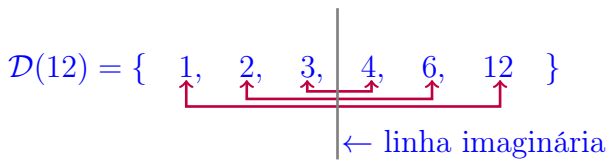
*Propriedade 6.* Se $p$ é primo então $\mathcal{D}(p) = \{1, p\}$.

Novamente fica para o estudante demonstrar essa propriedade.

*Propriedade 7.* Seja $n \neq 0$. Os elementos de $\mathcal{D}(n)$ podem ser organizados em dois grupos com a mesma quantidade, um constituído dos divisores $< \sqrt{n}$ e outro constituído dos divisores $> \sqrt{n}$. O número real $\sqrt{n}$ pode ser um divisor isolado fora desses dois grupos ou pode não ser um divisor.

De fato, seja $n = rs$, com $r \leq s$. Se $r = s$ então $n = r^2$ e $r = \sqrt{n}$ é um divisor de $n$. Suponhamos que $r < s$. Temos $r \cdot r < rs$ ou $r^2 < n$, ou seja, $r < \sqrt{n}$. Por outro lado $r < s \Rightarrow rs < s \cdot s \Rightarrow n < s^2$, ou seja, $\sqrt{n} < s$. Portanto, os divisores de $n$ ocorrem em pares, com um $< \sqrt{n}$ e outro $> \sqrt{n}$, exceto quando $n$ é um quadrado perfeito, sendo que nesse caso $\sqrt{n}$ é um divisor isolado, situado entre os dois grupos.

Colocando os elementos de $\mathcal{D}(n)$ em ordem crescente, podemos desenhar uma linha imaginária passando por $\sqrt{n}$, esteja ou não $\sqrt{n}$ em $\mathcal{D}(n)$, e observar claramente os dois grupos, como está ilustrado a seguir.

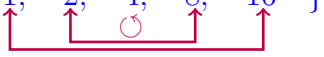


Vemos nesse exemplo que a linha imaginária passa por $\sqrt{12} \approx 3,46$, sendo que esse número não comparece em $\mathcal{D}(12)$ pelo motivo de não ser número natural.

*Propriedade 8.* Seja $n \neq 0$. Colocando os elementos de $\mathcal{D}(n)$ em ordem crescente, vemos que o produto de dois elementos quaisquer equidistantes dos extremos é sempre $n$. Fica subtendido que se houver um elemento central se faz o produto dele por ele mesmo, que assim é igual a $n$.

Os divisores de 12, exibidos logo acima, ilustram essa propriedade: $1 \cdot 12 = 12$, $2 \cdot 6 = 12$, $3 \cdot 4 = 12$. Examinando os divisores de 16 vemos um caso em que existe um elemento central: $4 \cdot 4 = 16$.

$$\mathcal{D}(16) = \{\ 1,\ 2,\ 4,\ 8,\ 16\ \}$$



Para justificar a propriedade basta observar o seguinte. Sejam $n = r_1 s_1$ e $n = r_2 s_2$, com $r_1 < r_2$. Multiplicando essa desigualdade por $s_1$ temos $s_1 r_1 < s_1 r_2$. Mas $s_1 r_1 = n = s_2 r_2$, de modo que $s_2 r_2 < s_1 r_2 \Rightarrow s_2 < s_1$. Portanto se ordenarmos de forma crescente os divisores $< \sqrt{n}$ a partir de 1, os respectivos quocientes (que são os divisores $> \sqrt{n}$) estão ordenados de forma decrescente a partir de $n$.

Podemos extrair da Propriedade 7 um importante resultado:

**Teorema 5.1.** *Se o número natural $n$ não é primo, então ele tem um divisor primo $\leq \sqrt{n}$.*

*Demonstração.* Se $n$ não é primo, existem números naturais $1 < r < n$ e $1 < s < n$ tais que $n = rs$. Podemos supor que $r \leq s$. Então $r^2 \leq rs = n$, portanto $r \leq \sqrt{n}$. Mas, de acordo com o Escólio 4.23, $r$ tem um divisor primo $p$, e temos $p \leq r$. Portanto $p \leq \sqrt{n}$. Por ser divisor de $r$, $p$ também é divisor de $n$, e terminamos. □

**Problema resolvido 5.2. a)** Explique por que, para todo número natural $m \geq 3$, o número $m^2 - 1$ é composto. **b)** Explique por que, para todo número natural $m \geq 3$, o número $m^2 - m - 2$ é composto. **c)** Prove que se $p \geq 5$ é primo, então o número $p^2 + 8$ é composto.

*Solução de a)* Como $m^2 - 1 = (m + 1)(m - 1)$ e como $m + 1 > 1$ e $m - 1 > 1$, então $m^2 - 1$ é composto. Note que a afirmação não é válida para $m = 1$ ou $m = 2$.

*Solução de b)* Todo trinômio do segundo grau $ax^2 + bx + c$ se decompõe na forma $ax^2 + bx + c = a(x - r)(x - s)$, sendo $r$ e $s$ os zeros do trinômio. Se $x$, $a$, $b$, $c$, $r$ e $s$ são números inteiros e se $x - r > 1$ e $x - s > 1$, então $ax^2 + bx + c$ é composto.

No caso em questão, os zeros de $m^2 - m - 2$ são 2 e $-1$, de modo que $m^2 - m - 2 = (m + 1)(m - 2)$. Se $m \geq 4$, temos $m + 1 > 1$ e $m - 2 > 1$, logo $m^2 - m - 2$ é composto. Se $m = 3$, temos $m^2 - m - 2 = 4$, que é composto.

*Solução de c)* A expressão $p^2 + 8$ é um trinômio do segundo grau. Assim, a princípio, podemos pensar em proceder como no item b). Mas as raízes desse trinômio são números complexos, de modo que aquela tática não funciona aqui. Assim devemos pensar em expressões para substituir $p$.

A primeira que pode ocorrer é considerar classes módulo 2. Assim, $p$ é par ou ímpar. Como $p$ é primo $\geq 5$, vemos que ele é ímpar. Podemos escrever $p = 2k + 1$ para algum número natural $k \geq 1$. Temos então $p^2 + 8 = (2k + 1)^2 + 8 = 4k^2 + 4k + 1 + 8 = 4k^2 + 4k + 9$. Novamente temos um trinômio do segundo grau cujas raízes são números complexos, de modo que novamente nossa tática não funcionou.

Podemos pensar em considerar classes módulo 3. Sabemos que $p$ se escreve na forma $3k$ ou $3k+1$ ou $3k+2$. Como $p$ é primo, a forma $3k$ só seria possível para $p=3$, mas, por hipótese $p \geq 5$. Ficamos assim com dois casos que devem ser examinados separadamente:

*1º caso:* $p = 3k+1$, com $k \geq 2$. Aqui $p^2+8 = (3k+1)^2+8 = 9k^2+6k+1+8 = 9k^2+6k+9 = 3(3k^2+2k+3)$, e $p^2+8$ se decompõe em dois fatores $> 1$. Vemos que é composto.

*2º caso:* $p = 3k+2$, com $k \geq 1$. Aqui $p^2+8 = (3k+2)^2+8 = 9k^2+12k+4+8 = 9k^2+12k+12 = 3(3k^2+4k+4)$, e novamente $p^2+8$ se decompõe em dois fatores $> 1$. Portanto é composto.

Fica provado que $p^2+8$ é composto para todo $p \geq 5$ primo.

Para encerrar, observe que a hipótese de $p$ ser primo é muito forte, bastaria supor que não é múltiplo de 3. Não fizemos isso porque ficaria muito óbvio que se deve considerar classes módulo 3. Por outro lado, $p^2+8$ é primo para vários valores ímpares de $p$ múltiplos de 3, como $p = 3$, 9, 15 e 21. □

**Problema resolvido 5.3. a)** Explique por que todo primo $p \geq 5$ é da forma $6q+1$ ou $6q+5$, para algum número natural $q$. **b)** Se $p$ é um primo $\geq 5$, então $p^2$ tem resto 1 quando dividido por 12. A recíproca é verdadeira?

*Solução de a)* $p$, assim como qualquer outro número natural, se escreve em uma das formas: $6k$, ou $6k+1$, ou $6k+2$, ou $6k+3$, ou $6k+4$, ou $6k+5$. Observemos primeiro que como $p$ é primo e $p \geq 5$ então $p$ é ímpar e não pode ser múltiplo de 3. Portanto $p$ não é das formas $6k$, $6k+2$, $6k+3$ ou $6k+4$. Assim só restam as formas $6q+1$ ou $6q+5$. Observamos que existem primos dessas formas, por exemplo, 7 e 11. Mas nem todo número de uma dessas formas é primo. Você pode dar exemplos. Existem infinitos primos da forma $6k+1$? E da forma $6k+5$?

*Solução de b)* Usando o item a) sabemos que $p = 6k+1$ ou $p = 6k+5$. Se $p = 6k+1$ temos $p^2 = (6k+1)^2 = 36k^2+12k+1 = 12(3k^2+k)+1$. Se $p = 6k+5$ temos $p^2 = (6k+5)^2 = 36k^2+60k+25 = 36k^2+60k+24+1 = 12(3k^2+5k+2)+1$. De qualquer forma $p^2$ tem resto 1 quando dividido por 12.

Quanto à recíproca de b), não é verdadeira (se fosse, seria muito fácil achar números primos, mas já estamos desconfiados de que não é assim!). Para encontrar exemplos, notemos que se $n$ tem resto 1 quando dividido por 12, então $n^2$ também tem. Assim basta tomar tais $n$ que não sejam primos, como $25 = 2 \cdot 12 + 1$, $49 = 4 \cdot 12 + 1$, etc. □

**Problema resolvido 5.4.** Certo número natural é múltiplo simultaneamente de 2, 3 e 5. Justifique por que ele é múltiplo de 30.

*Solução 1.* Seja $n$ um número natural múltiplo simultaneamente de 2, 3 e 5. Usando o resultado do Problema 4.10.25, já sabemos que $n$ é múltiplo de 6, de modo que podemos escrever $n = 6q$ para algum número natural $q$. Observe que se conseguirmos justificar que $q$ é múltiplo de 5, poderemos concluir, pois $q = 5t \Rightarrow n = 6 \cdot 5t = 30t$.

Para ver que $q$ deve ser múltiplo de 5 usamos classes módulo 5:

*1ª. possibilidade:* $q = 5l+1$. Nesse caso $n = 6q = 6(5l+1) = 30l+6 = 5(6l+1)+1$ não é múltiplo de 5, e assim essa possibilidade não ocorre.

*2ª. possibilidade:* $q = 5l+2$. Da mesma forma se mostra que não ocorre.

*3ª. possibilidade:* $q = 5l+3$. Da mesma forma se mostra que não ocorre.

*4ª. possibilidade:* $q = 5l+4$. Da mesma forma se mostra que não ocorre.

*5ª. possibilidade:* $q = 5l$. Como é a última possibilidade, ela é a que ocorre, e assim terminamos.

*Solução 2.* Sai mais rápido se você começar escrevendo $n = 5q$. Experimente. □

## 5.3 Problemas

**Problema 5.3.1.** Justifique as Propriedades 5 e 6 enunciadas no texto.

**Problema 5.3.2.** Seja $n \neq 0$. Explique por que se $\sqrt{n}$ for um número natural então é um divisor de $n$, e, se não for número natural, não é divisor. E por que no primeiro caso $n$ tem uma quantidade ímpar de divisores, e no segundo caso, essa quantidade é par.

**Problema 5.3.3.** Responda e justifique:

**a)** Se $n > 1$ e se $\mathcal{D}(n) = \{1, n\}$ então $n$ é _____

**b)** Se $1 < m < n$ são três elementos de $\mathcal{D}(n)$, outro possível elemento é _____

**c)** Se $p$ é primo, os exemplos indicam que $\mathcal{D}(p^2) =$ _____

**d)** Se $p < q$ são primos, os exemplos indicam que $\mathcal{D}(pq) =$ _____

**e)** Se $p < q < r$ são primos, exemplos indicam que $\mathcal{D}(pqr) =$ _____

**f)** Se $n > 1$, o segundo menor elemento de $\mathcal{D}(n)$ com certeza é _____

**g)** Se $n > 1$, o terceiro menor elemento de $\mathcal{D}(n)$ (se existir) com certeza é _____ ou _____

**Problema 5.3.4.** Assinale V ou F dentro dos parêntesis se a afirmação for verdadeira ou falsa, respectivamente. Justifique.

( ) Se $n$ é ímpar e se $m \in \mathcal{D}(n)$ então $m$ é ímpar.

( ) Se $n$ é par e se $m \in \mathcal{D}(n)$ então $m$ é par.

( ) O menor múltiplo de qualquer número natural é 1.

( ) Sabendo-se de antemão que 73373 não é primo, então com certeza ele tem um divisor primo $p$ tal que $2 < p < 270$.

( ) O menor divisor de qualquer número natural par é 2.

**Problema 5.3.5.** Encontre o menor número natural $> 0$ que é mútiplo simultaneamente de 2, 3, 4, 5, 6, 7, 8 e 9. Você tem uma justificativa?

**Problema 5.3.6.** Quantos números naturais de 104 a 995 são múltiplos de 7?

**Problema 5.3.7.** **a)** Como são os múltiplos simultâneos de 4 e de 5? **b)** Encontre a soma de todos os números de 1 a 1000 que são múltiplos de 4 e de 5.

**Problema 5.3.8.** Encontre a soma de todos os números de 1 a 100 que não são múltiplos de 4 ou de 5.

**Problema 5.3.9.** Seja $n$ um número natural qualquer. Foi visto no Capítulo 4 que, se 3 é divisor de $n^2$, então 3 é divisor de $n$ e 9 é divisor de $n^2$. **a)** Explique por que, se 5 é divisor de $n^2$, então 5 é divisor de $n$ e 25 é divisor de $n^2$. **b)** Dê exemplos de $n$ tais que 4 é divisor de $n^2$ mas 4 não é divisor de $n$ e $4^2$ não é divisor de $n^2$.

**Problema 5.3.10.** Quantos quadrados perfeitos existem entre 40000 e 640 000 que são múltiplos simultaneamente de 3, 4 e 5?

**Problema 5.3.11.** Seja $x$ o menor de três números naturais positivos cujo produto é 720. Encontre o maior valor possível de $x$.

**Problema 5.3.12.** Explique por que 1 é o único número $n$ com um dígito tal que todos os números $10n+1$, $10n+3$, $10n+7$ e $10n+9$ são primos.

**Problema 5.3.13.** Explique por que 2 é o único primo da forma $n^n+n$ para todo número natural $n \geq 1$.

**Problema 5.3.14.** Explique por que o único primo da forma $n^3-1$ é 7, qualquer que seja o número natural $n$.

**Problema 5.3.15.** Investigue quais são os primos $p$ e $q$ para os quais $p-q$ também é primo.

*Solução.* Examinando alguns exemplos, um caso imediato que se observa é o seguinte. Suponhamos que $q$ e $q+2$ sejam primos gêmeos. Então, pondo $p=q+2$, temos que $p$, $q$ e $p-q=2$ são primos. Em outra ordem, $p$, 2 e $p-2=q$ são primos.

Em geral, sejam $p$, $q$ e $p-q$ primos. Temos que ter $p>q$ para que $p-q \geq 2$ seja primo. Assim, $p$ e $q$ não são ambos pares, pois isso implicaria $p=q=2$. Se $p$ e $q$ são ambos ímpares, então $p-q$ é um primo par, logo $p-q=2$, e $p=q+2$, de modo que $p$ e $q$ são primos gêmeos. Por outro lado, se $p$ e $q$ não são ambos ímpares, então $q=2$, e $p-q=p-2$ é primo. Portanto $p$ e $p-q$ são primos gêmeos.

Em resumo, se $p$, $q$ e $r=p-q$ são primos então $p=q+2$ e $q$ são primos gêmeos com $r=2$, ou $p=r+2$ e $r$ são primos gêmeos com $q=2$.

Não se sabe se existem infinitos primos gêmeos, mas existe uma grande quantidade de exemplos.

**Problema 5.3.16.** Explique por que para todo número natural $n \geq 2$ não existe primo entre $n!+2$ e $n!+n$, incluindo esses.

**Problema 5.3.17.** Explique por que qualquer função quadrática cujos coeficientes são todos primos não pode ter uma raiz dupla.

**Problema 5.3.18.** Demonstre que 8, 10 e todo número natural $n>11$ pode ser escrito como soma de dois números compostos.

**Problema 5.3.19.** Verifique que se $n<p^3$ para todo divisor primo $p$ de $n$ então $n$ é primo ou produto de dois primos.

**Problema 5.3.20. a)** Explique por que $p^2+m$ é composto para todo primo $p \geq 3$ e todo número natural ímpar $m$. **b)** Explique por que para todo número natural $m \geq 3$ o número $2m^2+m-6$ é composto. **c)** Verifique que se $p \geq 5$ é primo então $p^2+2$ é composto. **d)** Nos itens a) e c), a hipótese de $p$ ser primo pode ser substituída por hipóteses mais fracas?

**Problema 5.3.21.** Explique por que se 3 é divisor de $2p$, com $p$ primo, então $p=3$.

**Problema 5.3.22.** Observe a decomposição em fatores primos de $288 = 2\cdot2\cdot2\cdot2\cdot2\cdot3\cdot3 = 2^5\cdot3^2$. Existem outros primos (diferentes de 2 e de 3) que dividem 288? Tente uma justificativa algébrica.

*Solução algébrica.* Um caminho pode ser o seguinte. Seja $p>2$ um divisor primo de 288. Escrevemos $288=pr$. Como $p$ é ímpar, $r$ é par, digamos $r=2s$. Logo $288=pr=p(2s)=2ps \Rightarrow 144=ps$. Novamente $s=2t \Rightarrow 144=p(2t) \Rightarrow 72=pt$. De novo $t$ é par e $t=2u \Rightarrow 72=p(2u)=2pu \Rightarrow 36=pu$. Novamente $u=2w \Rightarrow 36=p(2w)=2pw \Rightarrow 18=pw$. Finalmente $w=2x \Rightarrow 9=px$. Como $p$ é primo e divide 9, só pode ser $p=3$ (é fácil ver,

exaurindo tentativas, que 3 é o único primo que é divisor de 9). Portanto $x = 3$ e 288 só tem dois divisores primos, que são 2 e 3.

*Solução braçal.* Arrume uma lista dos primos $< 288$ e faça todas as divisões. Na verdade basta considerar os primos até 144, pois entre $288/2$ e 288 não existem divisores. Você encontra uma lista de primos no Apêndice A. □

Considere os números $2^j$, para algum número natural $j \geq 1$ fixado. Certamente que os números 1, 2, $2^2$, ..., $2^{j-1}$ e $2^j$ são seus divisores. Existem outros divisores? Para compreender esse tipo de situação estude os problemas seguintes.

**Problema 5.3.23.** Seja $a$ um número natural $\geq 2$, e sejam $m$ e $n$ números naturais. Demonstre que $a^m$ divide $a^n$ se e somente se $m \leq n$. Conclua que 1, 2, $2^2$, ..., $2^{j-1}$ e $2^j$ são as únicas potências de 2 que são divisores de $2^j$.

**Problema 5.3.24.** Consideremos as potências $2^j$ de 2, para $j \geq 1$. Podem ser números bem grandes, por exemplo, $2^{40} = 1\,099\,511\,627\,776$. **a)** Mostre que, para todo número natural $n$, existe um número natural $t$ tal que $n < 2^t$. Em outra linguagem, isso significa que $2^t \to +\infty$. **b)** Esses números, assim com qualquer outro número natural, é um produto de primos. Certamente que 2 é um deles. Podem haver outros? Quais são os divisores de $2^j$? Crie um argumento para justificar sua resposta.

**Problema 5.3.25.** Encontre, justificando detalhadamente, todos os divisores de $3^j$ para todo $j \geq 1$. Existem outros primos, além de 3, que dividem $3^j$ ?

**Problema 5.3.26.** Sobre o número natural $n = 2^3 3^m$ sabe-se que ele tem 28 divisores. Qual o valor de $n$? Justifique detalhadamente.

## 5.4 Reconhecimento dos primos

Se um número natural $b \neq 0$ é divisor do número natural $a$, então existe um número natural $q$ tal que $a = bq$. Portanto se os números $a$ e $b$ estão representados em um sistema de numeração posicional podemos dividir $a$ por $b$ usando o algoritmo usual de divisão, e desse cálculo resulta quociente $q$ e resto zero:

$$\begin{array}{r|l} a & b \\ \hline 0 & q \end{array}$$

Por outro lado, se do algoritmo usual de divisão resultar resto $r \neq 0$, então $b$ não é divisor de $a$.

Seja então um número natural $n \geq 2$, representado no sistema decimal, cuja primaridade queremos verificar. De acordo com a definição de primo, necessitamos dividir $n$ por todos os números naturais $\geq 2$ e $< n$. Se alguma dessas divisões for exata, encontramos um divisor e $n$ não é primo. Se nenhuma divisão for exata, então $n$ é primo.

Podemos fazer muita economia nesses cálculos lembrando que se um número $n$ é composto então ele tem um divisor $\leq \sqrt{n}$. Observamos também que se $n$ for par $> 2$ então $n$ não é primo, e se $n$ for ímpar então não é múltiplo de nenhum número par. Ainda, se $n$ não for múltiplo de 3 então ele não é múltiplo de nenhum outro múltiplo de 3, o mesmo para 5, 7, e assim por diante.

Em resumo, um método elementar para verificar se $n > 5$ é primo é o seguinte: vemos primeiro se $n$ é par, múltiplo de 3 ou de 5. Se isso ocorrer sabemos que $n$ é composto. Caso contrário, dividimos $n$ por todos os ímpares de 7 a $\sqrt{n}$ que não são múltiplos de 3 ou de 5. Se nenhuma divisão for exata, então $n$ é primo.

O método mais econômico aqui é lembrar que se $n$ for composto, então, em virtude do Teorema 5.1, ele tem um divisor primo $\leq \sqrt{n}$. Entretanto para aplicar isso necessitamos dispor de uma lista de números primos $\leq \sqrt{n}$. Podemos obter listas de números primos usando o crivo de Eratóstenes, o qual explicaremos na seção seguinte, ou utilizando uma lista de primos previamente construída, como a do Apêndice A.

Lembramos que existem muitos aplicativos computacionais algébricos munidos de algoritmos de primaridade muito rápidos e que respondem quase que de imediato se um dado número (de um tamanho não muito excepcional) é primo ou não. Que tal você mesmo construir alguns desses aplicativos? Para isso estamos investigando, começando com os algoritmos mais básicos.

**Problema resolvido 5.5.** Verificar a primaridade de 157.

*Solução.* Como $\sqrt{157} \approx 12,53$, basta, a princípio, dividir 157 por todos os números $\geq 2$ e $\leq 12$. Para economizar esforço observamos logo que 157 não é par e não é múltiplo de 3 ou de 5. Assim basta dividi-lo pelos ímpares de 1 a 12 que não são múltiplos de 3 ou de 5. Sobraram apenas 7 e 11. Temos

$$\begin{array}{rr|l} 157 & 7 & \\ \cline{2-2} 17 & 22 & \\ 3 & & \end{array} \qquad \begin{array}{rr|l} 157 & 11 & \\ \cline{2-2} 47 & 14 & \\ 3 & & \end{array}$$

Como nenhuma divisão é exata, 157 é primo. □

**Problema resolvido 5.6.** Verificar a primaridade de 287.

*Solução.* Calculamos primeiro $\sqrt{287} \approx 16,94$. Em seguida observamos que 287 não é par e não é múltiplo de 3 ou de 5. Assim basta dividi-lo pelos ímpares de 1 a 16 que não são múltiplos de 3 ou de 5. Sobraram 7, 11 e 13. Temos

$$\begin{array}{rr|l} 287 & 7 & \\ \cline{2-2} 07 & 41 & \\ 0 & & \end{array}$$

Como deu resto zero podemos parar as divisões pois já sabemos que 287 não é primo e que 7 é um fator. □

**Problema resolvido 5.7.** Verificar a primaridade de 1811.

*Solução.* Como $\sqrt{1811} \approx 42,55$, basta dividir 1811 por todos os números $\geq 2$ e $\leq 42$. Como 1811 não é par e não é múltiplo de 3 ou de 5, basta dividi-lo por 7, 11, 13, 17, 19, 23, 29, 31, 37 e 41. Temos

$$\begin{array}{rr|l} 1811 & 7 & \\ \cline{2-2} 41 & 258 & \\ 61 & & \\ 5 & & \end{array} \qquad \begin{array}{rr|l} 1811 & 11 & \\ \cline{2-2} 71 & 164 & \\ 51 & & \\ 7 & & \end{array} \qquad \begin{array}{rr|l} 1811 & 13 & \\ \cline{2-2} 51 & 139 & \\ 121 & & \\ 4 & & \end{array} \qquad \begin{array}{rr|l} 1811 & 17 & \\ \cline{2-2} 111 & 106 & \\ 9 & & \end{array}$$

| 1811 | 19 |
|---|---|
| 101 | 95 |
| 6 | |

| 1811 | 23 |
|---|---|
| 201 | 78 |
| 17 | |

| 1811 | 29 |
|---|---|
| 71 | 62 |
| 13 | |

| 1811 | 31 |
|---|---|
| 261 | 58 |
| 13 | |

| 1811 | 37 |
|---|---|
| 331 | 48 |
| 35 | |

| 1811 | 41 |
|---|---|
| 171 | 44 |
| 7 | |

Como nenhuma divisão é exata, 1811 é primo. □

## 5.5 Problemas

**Problema 5.5.1.** Verifique se são primos ou não os números seguintes. Se algum deles não for primo, encontre o menor número primo que o divide. **a)** 179; **b)** 819; **c)** 1153; **d)** 6851.

**Problema 5.5.2.** Verifique que 38567 é primo.

**Problema 5.5.3.** Alguns números têm todo "jeito" de serem primos. Examinando cada número da lista a seguir, diga de imediato se acha que ele é primo ou não. Depois confirme usando algum recurso de primaridade.

$$119, \quad 203, \quad 713, \quad 817, \quad 1219, \quad 1513.$$

**Problema 5.5.4.** Encontre todos os números primos que se escrevem com três dígitos decimais e tais que o produto de seus dígitos também é primo.

**Problema 5.5.5.** Estude e justifique o seguinte teste de primaridade para $n \geq 9$ ímpar: dividir $n$ pelos ímpares 3, 5, 7, ..., $n$, nessa ordem, parando as divisões quando encontrar um quociente menor do que o divisor; se não houve divisão anterior exata então $n$ é primo.

*Solução.* O estudante pode aplicar o teste para alguns números, por exemplo, 331 e 701. Quanto à justificativa, vejamos.

Se $n \geq 9$ é um ímpar composto, podemos escrever $n = ab$, sendo $a > 1$ e $b > 1$ e $a \leq b$. Como $n$ é ímpar, segue que $a$ é ímpar. Em outros termos, se $n \geq 9$ é um ímpar composto, existe um divisor ímpar $a$ e um quociente $b$ tais que $3 \leq a \leq b$.

Portanto, se dividirmos $n$ por $a = 3, 5, 7, \ldots$, nessa ordem, enquanto o divisor é menor ou igual ao quociente, e todas as divisões forem não exatas, o número $n$ é primo. □

*Observação.* O presente critério de primaridade é equivalente àquele dado no texto, em que procuramos divisores $\leq \sqrt{n}$. De fato, se encontramos um divisor $a$ tal que $n = ab$ com $a \leq b$, então $a^2 \leq ab = n$, o que implica $a \leq \sqrt{n}$. E se encontramos um divisor $a \leq \sqrt{n}$, e se $b$ é o quociente com $n = ab$, temos $a^2 \leq n = ab$, o que implica $a \leq b$.

**Problema 5.5.6.** O algoritmo de primaridade do problema anterior pode ser desenvolvido na forma de um procedimento: dado $n \geq 3$ ímpar, dividir $n$ pelos ímpares 3, 5, 7, ... seguindo a ordem crescente dessa sequência, enquanto (i) os quocientes das divisões forem maiores ou iguais aos divisores, e (ii) o resto da divisão for não nulo.
**a)** Observe que o procedimento tem dois critérios de parada: $(i')$ para quando encontra um divisor maior do que seu quociente; ou $(ii')$ para quando uma divisão for exata. Explique por que se o critério de parada utilizado foi $(i')$ então $n$ é primo, e se foi $(ii')$, então $n$ é composto. **b)** Aplique e verifique o algoritmo para todos os números naturais ímpares $n$ tais que $3 \leq n \leq 31$. **c)** Aplique o algoritmo dado para verificar se 911 é primo ou não.

**Problema 5.5.7.** Dado um algoritmo de primaridade $\mathcal{A}$ e dado um número natural $n$, indicaremos por $\mathcal{A}(n)$ a quantidade máxima de divisões necessárias para, usando o algoritmo $\mathcal{A}$, determinar se $n$ é primo ou não. Para todo número natural ímpar $n \geq 5$ calcule $\mathcal{A}(n)$ para os seguintes algoritmos de primaridade: **a)** dividir $n$ pelos ímpares 3, 5, 7, ..., $n-2$; se nenhuma das divisões for exata, então $n$ é primo. **b)** dividir $n$ pelos ímpares 3, 5, 7, ..., $n-2$, nessa ordem, até encontrar um quociente maior do que o divisor; se nenhuma das divisões for exata, então $n$ é primo. **c)** Usando o algoritmo anterior, quantas divisões você precisaria fazer, no máximo, para verificar se $n = 1\,000\,003$ é primo ou não?

## 5.6 O crivo de Eratóstenes

Eratóstenes de Cirene propôs, por volta de 200 a.C., um método de obtenção da lista dos números primos até um limite pré-estabelecido. Esse método passou a ser denominado *crivo de Eratóstenes*. Explicamos a seguir como ele é implementado.

Listamos os números naturais com o intuito de eliminar da lista os que não são primos. Nossa lista contém ordenadamente os números naturais de 2 até um determinado número $n$.

2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, ...

O primeiro da lista, a saber, 2, é primo, pois não existe antes dele número $> 1$ que possa ser seu divisor. Todo múltiplo de 2 (exceto ele mesmo) não é primo, e deve ser eliminado da lista. Eliminamos um número da lista crivando-o com riscos, como segue.

2, 3, ~~4~~, 5, ~~6~~, 7, ~~8~~, 9, ~~10~~, 11, ~~12~~, 13, ~~14~~, 15, ~~16~~, 17, ~~18~~, 19, ~~20~~, 21, ~~22~~, 23, ...

Portanto, crivamos na lista os pares, exceto 2. O primeiro da lista, após 2, que não foi crivado é 3. Ele é primo, pois se fosse composto seria múltiplo de algum número $< 3$ e já teria sido crivado. Todo múltiplo de 3 (exceto ele mesmo) não é primo, e deve ser eliminado da lista. É o que fazemos a seguir.

2, 3, ~~4~~, 5, ~~6~~, 7, ~~8~~, ~~9~~, ~~10~~, 11, ~~12~~, 13, ~~14~~, ~~15~~, ~~16~~, 17, ~~18~~, 19, ~~20~~, ~~21~~, ~~22~~, 23, ...

O primeiro da lista, após 3, que não foi crivado é 5, que é primo, pois se fosse composto seria múltiplo de algum número $< 5$ e já teria sido crivado. Todo múltiplo de 5 (exceto ele mesmo) não é primo, e deve ser eliminado da lista. Repetimos esse procedimento prosseguindo até o final da lista. Dessa forma eliminamos qualquer número composto, permanecendo apenas os primos.

Para exemplificar listamos abaixo os números naturais de 2 a 50 e aplicamos o método do crivo:

2, 3, ~~4~~, 5, ~~6~~, 7, ~~8~~, ~~9~~, ~~10~~, 11, ~~12~~, 13, ~~14~~, ~~15~~, ~~16~~, 17, ~~18~~, 19, ~~20~~, ~~21~~, ~~22~~, 23, ~~24~~, ~~25~~, ~~26~~, ~~27~~, ~~28~~, 29, ~~30~~, 31, ~~32~~, ~~33~~, ~~34~~, ~~35~~, ~~36~~, 37, ~~38~~, ~~39~~, ~~40~~, 41, ~~42~~, 43, ~~44~~, ~~45~~, ~~46~~, 47, ~~48~~, ~~49~~, ~~50~~.

Os números não riscados dessa lista são os números primos $\leq 50$:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47.

Vemos assim como o método do crivo de Eratóstenes nos fornece uma maneira prática de obter os números primos menores do que ou iguais a um dado número natural. Para aplicação do método a lista dos números naturais pode ser organizada em uma tabela de várias formas, e vemos a seguir uma dessas formas em que consideramos 100 como o número limite.

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 |
| 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 |
| 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 | 49 | 50 |
| 51 | 52 | 53 | 54 | 55 | 56 | 57 | 58 | 59 | 60 |
| 61 | 62 | 63 | 64 | 65 | 66 | 67 | 68 | 69 | 70 |
| 71 | 72 | 73 | 74 | 75 | 76 | 77 | 78 | 79 | 80 |
| 81 | 82 | 83 | 84 | 85 | 86 | 87 | 88 | 89 | 90 |
| 91 | 92 | 93 | 94 | 95 | 96 | 97 | 98 | 99 | 100 |

O estudante poderá reproduzir essa tabela em uma folha de escrever (ou imprimir esta página) e implementar o procedimento proposto, obtendo os números primos $\leq 100$.

Descrevemos novamente o algoritmo observando em acréscimo algumas propriedades.

**i)** 2 é primo pois não existe número $> 1$ antes dele que possa ser seu divisor. Em seguida crivamos os múltiplos $2q$ de 2 para $q > 1$, o primeiro é 4. Para crivar os múltiplos de 2 basta percorrer a lista crivando um sim outro não a partir de 4. Isto é, crivamos contando de dois em dois.

**ii)** O primeiro não crivado é 3, que assim é primo (se fosse composto seria múltiplo de algum número antes dele e já teria sido crivado). Crivamos os múltiplos $3q$ para $q > 1$, o primeiro ainda não crivado é 9. Para crivar os múltiplos de 3 basta percorrer a lista crivando um sim e dois não a partir de 9. Isto é, crivamos contando de três em três.

**iii)** O primeiro não crivado é 5, que assim é primo (se fosse composto seria múltiplo de algum número antes dele e já teria sido crivado). Crivamos os múltiplos $5q$ para $q > 1$, o primeiro ainda não crivado é 25. Crivamos contando de cinco em cinco.

**iv)** O primeiro não crivado é 7, que assim é primo. Crivamos os múltiplos $7q$ para $q > 1$, o primeiro ainda não crivado é 49. Crivamos contando de sete em sete.

Continuamos repetindo esse procedimento até acabar a lista.

Observamos que, ao iniciar a eliminação dos múltiplos de um primo $p$, o primeiro que ainda não foi crivado é $p^2$. De fato, dado um múltiplo de $p$ da forma $sp$, com $2 \leq s < p$, sabemos que $s$ tem divisor primo, logo $sp$ é múltiplo de um primo $< p$, e já foi crivado.

Essa observação nos fornece um critério de parada na execução do método. Ao iniciar a eliminação dos múltiplos de um primo $p$, examinamos $p^2$. Se esse número não estiver na tabela, então nada mais é necessário eliminar, e o método está concluído. Em outros termos, ao aplicar o método do crivo em uma tabela de números de 1 a $n$, basta eliminar os múltiplos $\geq p^2$ dos primos $p$ tais que $p \leq \sqrt{n}$.

No caso da lista dos números de 1 a 100, aplicamos o método eliminando os múltiplos dos primos 2, 3, 5 e 7 (exceto eles mesmos). O primo seguinte é 11. Como $11^2 = 121$ não se encontra na lista, paramos a crivagem. Tomamos os números não crivados, que são os primos até 100. O estudante que aplicou o crivo nessa tabela pode conferir os primos obtidos com os da lista na página 243.

Na implementação do método do crivo, várias economias podem ser feitas. Por exemplo, na tabela acima de números de 2 a 100, não precisamos escrever os pares e nem os múltiplos de 5. Restam assim apenas quatro colunas. Na lista final de primos não se deve esquecer de acrescentar 2 e 5.

O método do crivo, além de fornecer uma lista de primos, nos proporciona uma maneira de encontrar todos os primos divisores de um dado número natural $n$, e também nos possibilita calcular a decomposição canônica de $n$. Adicionalmente, podemos listar todos os divisores de $n$ (primos ou não). Vejamos um exemplo.

**Problema resolvido 5.8. a)** Encontre todos os primos divisores de 539. **b)** Encontre a decomposição canônica de 539. **c)** Liste todos os divisores de 539.

*Solução de a)* Notando que 539 não é par e nem é múltiplo de 3 ou de 5, organizamos os números de 3 a 539 em uma tabela. Aplicamos o método do crivo, anotando os primos que crivam 539. Para obter todos os divisores primos de 539, não aplicamos o critério de parada "$p^2$". No caso os primos divisores de 539 são 7 e 11.

*Solução de b)* Como $7 \cdot 11 = 77$, ainda não temos a decomposição procurada. Notando que $539/77 = 7$, vemos que 539 é divisível por $7^2$. Conferindo, temos $539 = 7^2 \cdot 11$, que é assim a decomposição canônica de 539.

*Solução de c)* Todo divisor de 539, exceto 1, tem 7 ou 11 como fator primo, sendo que 7 pode aparecer duas vezes. Portanto os divisores de 539 são:

$$1, \qquad 7, \qquad 11,$$

$$7 \cdot 7, \qquad 7 \cdot 11,$$

$$7 \cdot 7 \cdot 11.$$

□



Figura 5.1. Desenho representativo de Eratóstenes de Cirene (c. 230 a.C.). Foi um dos dirigentes da antiga biblioteca de Alexandria, e contribuiu com descobertas em vários campos da ciência, como Astronomia, Geografia e Matemática. Seu mais famoso feito foi determinar um valor aproximado para o raio da Terra utilizando Geometria Euclidiana e os raios do Sol.

## 5.7 Problemas

**Problema 5.7.1.** Ao implementar o crivo de Eratóstenes para a tabela de números de 2 a 100 disposta no texto acima, coloque sua atenção nos momentos em que 91 é crivado. Dessa forma você pode encontrar os primos que dividem 91, assim como sua decomposição canônica.

**Problema 5.7.2. a)** Obtenha a lista dos números primos $\leq 300$ usando o método do crivo. Ao implementar o crivo esteja atento à pergunta seguinte. **b)** Encontre todos os primos que são divisores de 273, assim como sua decomposição canônica. **c)** Liste todos os divisores de 273.

**Problema 5.7.3.** Observe a seguinte tabela de números naturais, listados em seis colunas:

| | | | | | |
|---|---|---|---|---|---|
| | 2 | 3 | 4 | 5 | 6 |
| 7 | 8 | 9 | 10 | 11 | 12 |
| 13 | 14 | 15 | 16 | 17 | 18 |
| 19 | 20 | 21 | 22 | 23 | 24 |
| 25 | 26 | 27 | 28 | 29 | 30 |
| 31 | 32 | 33 | 34 | 35 | 36 |
| 37 | 38 | 39 | 40 | 41 | 42 |

**a)** Aplique o método do crivo a essa tabela. Observe que os números primos, com exceção de 2 e 3, encontram-se em duas colunas apenas. Isso continua ocorrendo mesmo se aumentarmos indefinidamente a tabela? Qual a explicação? **b)** Para aproveitar melhor o espaço de uma folha, faça uma tabela de números naturais listados em doze colunas. Em quais colunas aparecem os números primos (com possíveis exceções)? Como você descreve essas colunas?

**Problema 5.7.4.** Ao fazermos uma lista de números naturais com o intuito de aplicar o método do crivo, podemos omitir os pares, e assim economizar algum esforço. **a)** Aplique o método do crivo à seguinte tabela:

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | 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 |

Ao listar os números primos assim obtidos, não se esqueça de acrescentar o primo 2.
**b)** Na tabela acima, para crivar os múltiplos de um primo $p$, podemos, a partir de $p^2$, contar de $p$ em $p$. Explique por que esse estratagema funciona.

**Problema 5.7.5.** Encontre uma decomposição em fatores primos de: **a)** 120; **b)** 375; **c)** 539; **d)** 2015; **e)** 1 455 521.

**Problema 5.7.6.** Encontre os divisores de: **a)** 120; **b)** 375; **c)** 539; **d)** 2015; **e)** 1 455 521.

**Problema 5.7.7.** Ao descrever o crivo de Eratóstenes, foi dito no texto que, ao começar a crivar os múltiplos $> p$ de um primo $p$, o primeiro ainda não crivado é $p^2$. Suponha $p \geq 3$. O próximo múltiplo depois de $p^2$ já foi crivado? E quantos aos seguintes, o que se pode dizer?

## 5.8 Infinitude dos primos

Uma das mais importantes propriedades que devemos investigar sobre os números primos é sua finitude ou infinitude. Existe uma quantidade finita ou infinita de primos?

A resposta a essa pergunta determina todo o procedimento futuro em nossas pesquisas sobre os números primos. Se existir uma quantidade finita de primos podemos ver se é possível listá-los, e assim, por inspeção, determinar todas as suas propriedades, e por extensão determinar propriedades dos números naturais. Por outro lado, se sua quantidade for infinita precisaremos usar procedimentos mais criativos para investigá-los.

Embora existam infinitos números naturais, isso não implica que existem infinitos primos. De fato, com uma quantidade finita de primos podemos fabricar infinitos números naturais.

Por exemplo, o primo 2 gera os números $2^j$, e os primos 2 e 3 geram $2^j 3^i$, com $j \geq 0$ e $i \geq 0$ naturais. Assim, a princípio, poderia ocorrer que uma quantidade finita de primos gerassem todos os números naturais.

Os matemáticos da Antiga Grécia conheciam a resposta à questão da finitude ou infinitude dos primos: existem infinitos números primos. Euclides, em *Os Elementos*, apresenta uma demonstração para esse fato. É muito importante para o estudante compreender o argumento de Euclides. Estude-o detalhadamente.

**Teorema 5.9** (Euclides)**.** *Existem infinitos números primos.*

*Demonstração.* Consideremos uma quantidade finita de primos, digamos $p_1$, $p_2$, ..., $p_n$, com $n \geq 1$. Com esses primos tomamos o número natural $A = p_1 p_2 \dots p_n + 1$. Como $A > 1$, o Teorema 4.22 garante que $A$ tem um divisor primo $p$. Portanto se dividirmos $A$ por $p$ o resto é zero. Então $p$ não pode ser um dos primos $p_1$, $p_2$, ..., $p_n$ considerados inicialmente. De fato, se $p$ fosse um desses primos, a divisão de $A$ por $p$ teria resto 1, o que não ocorre.

Concluímos do exposto acima que, qualquer que seja o conjunto finito de números primos, sempre existe um primo que não está nesse conjunto. Isso significa que a quantidade de primos é infinita. □



Figura 5.2. Euclides de Alexandria (c. 300 a.C.) foi um dos mais importantes matemáticos da Antiga Grécia. Compilou grande parte da Matemática de seu tempo em sua obra *Os Elementos*, procurando apresentá-la de forma rigorosa. Em particular, em Geometria, desenvolveu um sistema axiomático, posteriormente popularizado com o nome Geometria Euclidiana. Incluiu em sua obra a Teoria dos Números, e demonstra a infinitude dos números primos no Livro IX, Proposição 20, com um argumento muito semelhante ao que usamos no Teorema 5.9.

Existem diversas demonstrações da infinitude dos primos. Uma coleção delas é apresentada no Capítulo 1 de [102]. Confira também nossa lista de problemas 5.9.

Existem ainda muitos resultados demonstrando a infinitude de números primos de um determinado formato. Por exemplo:

**Problema resolvido 5.10.** Existem infinitos números primos da forma $3n + 2$.

*Solução.* Exemplos de números primos da forma $3n+2$ são: 2, 5, 11, 17, etc. Consideremos uma quantidade finita de primos $> 2$ da forma $3n+2$, denominando-os $p_1$, $p_2$, ..., $p_m$. Consideremos o número $A = 3p_1 p_2 \dots p_m + 2$. De acordo com o Problema Resolvido 4.28 $A$ tem um fator primo $p$ da forma $3n + 2$. Como $A$ é ímpar temos $p > 3$. Se $p$ fosse um dos $p_i$ para algum $i$ isso implicaria que $p$ seria um divisor de $A - 3p_1 p_2 \dots p_m$, portanto de 2, o que não é possível. Segue que $p \neq p_i$ para todo $i$. Concluímos que dado qualquer conjunto finito de primos da forma $3n+2$ sempre existe um primo dessa forma fora do conjunto. Segue que existem infinitos primos da forma $3n + 2$. □

Johann Dirichlet demonstrou em 1837 o seguinte resultado mais geral: *Se $d \geq 2$ e $a \neq 0$ são números naturais sem fatores primos comuns, então a progressão aritmética $a$, $a + d$, $a + 2d, \dots$ contém uma infinidade de números primos.*



Figura 5.3. Johann Peter Gustav Lejeune Dirichlet (1805-1859) participou da importante escola de matemáticos alemães do século XIX. Foi estudante, professor e colega de grandes nomes da Matemática na Europa de seu tempo, principalmente na Alemanha e na França. Contribuiu para o desenvolvimento da Análise, Equações Diferenciais, Teoria das Séries, particularmente as de Fourier. Seu principal interesse era a Teoria dos Números.

## 5.9 Problemas

**Problema 5.9.1.** Existem infinitos primos da forma $6n + 5$?

**Problema 5.9.2.** No Teorema de Dirichlet enunciado logo acima, a condição de que "$d \geq 2$ e $a \neq 0$ não têm fatores primos comuns" é sempre necessária?

**Problema 5.9.3.** **a)** Explique por que se $m > 1$ e $n$ são números naturais tais que $m$ divide $n! + 1$ então $m > n$. **b)** Conclua que para todo número natural $n$ existe um primo $p$ tal que $p > n$. **c)** Use esse resultado para dar outra demonstração (diferente da do texto) de que existem infinitos números primos. Segundo o autor de [102], página 3, essa demonstração é atribuída a Charles Hermite.

**Problema 5.9.4.** Complete os detalhes da seguinte variante da demonstração de Euclides da infinitude dos números primos. Se $A = p_1 p_2 \dots p_n$ e se $p$ é um primo que divide $A - 1$ então $p \neq p_i$ para todo $i$. Essa demonstração foi observada por Ernst Kummer (confira [102], página 3).

**Problema 5.9.5.** Demonstre que existem infinitos primos da forma $4n + 3$ (naturalmente sem utilizar o Teorema mais geral de Dirichlet).

**Problema 5.9.6.** Vamos denominar o $n$-ésimo número primo por $p_n$. Portanto $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, etc. Inspirados na demonstração de Euclides da infinitude dos primos, consideremos os números naturais $E_n = p_1 p_2 p_3 \dots p_n + 1$. Se $E_n$ é primo, dizemos que é um *primo de Euclides*. Comprove que $E_n$, para $1 \leq n \leq 5$, são primos de Euclides, mas $E_6$, $E_7$ e $E_8$ não são.

Não se sabe se existem infinitos primos de Euclides.

## 5.10 O máximo divisor comum

O exame dos divisores comuns de dois ou mais números naturais pode nos revelar sua natureza recíproca. Particularmente importante é o maior divisor comum.

Dado um número natural $a$, continuamos indicando por $\mathcal{D}(a)$ o conjunto dos divisores de $a$. Já observamos que 1 está em $\mathcal{D}(a)$ qualquer que seja $a$, e que $\mathcal{D}(a)$ é finito se $a \neq 0$. Portanto, dados números naturais $a$ e $b$ não simultaneamente nulos o conjunto $\mathcal{D}(a) \cap \mathcal{D}(b)$ é não vazio e finito. Segue que $\mathcal{D}(a) \cap \mathcal{D}(b)$ tem um elemento máximo. Isso justifica a seguinte definição.

**Definição 5.11.** Dados números naturais $a$ e $b$ não simultaneamente nulos o elemento máximo do conjunto $\mathcal{D}(a) \cap \mathcal{D}(b)$ chama-se *máximo divisor comum* de $a$ e $b$, e é indicado por $\text{mdc}(a, b)$. Se $a = 0$ e $b = 0$ convém definir $\text{mdc}(0, 0) = 0$.

As mesmas observações se aplicam para três ou mais números naturais $a_1$, $a_2$, ..., $a_n$, e da mesma forma se define $\text{mdc}(a_1, a_2, \ldots, a_n)$. Mais precisamente, se $a_1$, $a_2$, ..., $a_n$ são números naturais não simultaneamente nulos, definimos $\text{mdc}(a_1, a_2, \ldots, a_n)$ como o maior elemento do conjunto $\mathcal{D}(a_1) \cap \ldots \cap \mathcal{D}(a_n)$. Caso contrário, definimos $\text{mdc}(0, 0, \ldots, 0) = 0$.

**Exemplo 5.12.** $\mathcal{D}(12) = \{1, 2, 3, 4, 6, 12\}$ e $\mathcal{D}(18) = \{1, 2, 3, 6, 9, 18\}$. Portanto $\mathcal{D}(12) \cap \mathcal{D}(18) = \{1, 2, 3, 6\}$ e $\text{mdc}(12, 18) = 6$.

**Exemplo 5.13.** Observemos que $\mathcal{D}(15) = \{1, 3, 5, 15\}$, $\mathcal{D}(30) = \{1, 2, 3, 5, 6, 10, 15, 30\}$ e $\mathcal{D}(75) = \{1, 3, 5, 15, 25, 75\}$. Portanto

$$\mathcal{D}(15) \cap \mathcal{D}(30) \cap \mathcal{D}(75) = \{1, 3, 5, 15\} \text{ e } \text{mdc}(15, 30, 75) = 15.$$

Algumas propriedades do máximo divisor comum de fácil observação são as seguintes:

*Propriedade 1.* $\text{mdc}(a, b) = \text{mdc}(b, a)$ quaisquer que sejam os números naturais $a$ e $b$.

De fato, se $a = 0$ e $b = 0$ temos $\text{mdc}(a, b) = 0 = \text{mdc}(b, a)$. Se $a$ e $b$ não são simultaneamente nulos, então $\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(b) \cap \mathcal{D}(a)$ quaisquer que sejam os números naturais $a$ e $b$.

*Propriedade 2.* Se o número natural $a \neq 0$ é um divisor do número natural $b$ então $\text{mdc}(a, b) = a$.

De fato, $\mathcal{D}(a) \subset \mathcal{D}(b)$, do que segue $\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(a)$. Como $a$ é o maior elemento de $\mathcal{D}(a)$, temos $\text{mdc}(a, b) = a$.

*Propriedade 3.* $\text{mdc}(0, a) = a$ qualquer que seja o número natural $a$.

Se $a = 0$ temos $\text{mdc}(0, a) = 0 = a$. Suponhamos $a \neq 0$. Como $\mathcal{D}(0) = \{1, 2, 3, 4, \ldots\}$ temos $\mathcal{D}(0) \cap \mathcal{D}(a) = \mathcal{D}(a)$. Como $a$ é o maior elemento de $\mathcal{D}(a)$ segue a validade da propriedade.

*Propriedade 4.* Se $a$ e $b$ são números naturais não simultaneamente nulos então $mdc(a, b) \geq 1$.

O estudante pode se certificar da validade da Propriedade 4.

Uma situação que devemos destacar é que existem números que não têm divisores comuns $> 1$. Por exemplo, $\mathcal{D}(91) = \{1, 7, 13, 91\}$ e $\mathcal{D}(187) = \{1, 11, 17, 187\}$. Portanto $\mathcal{D}(91) \cap \mathcal{D}(187) = \{1\}$ e $\text{mdc}(91, 187) = 1$. Esses números recebem uma denominação especial.

**Definição 5.14.** Os números naturais $a$ e $b$ chamam-se *relativamente primos* quando $\text{mdc}(a, b) = 1$. Nesse caso $a$ e $b$ também são denominados *primos entre si* ou *coprimos*. Da mesma forma, se os números naturais $a_1$, $a_2$, ..., $a_n$ são tais que $\text{mdc}(a_1, a_2, \ldots, a_n) = 1$, dizemos que são relativamente primos (ou primos entre si, ou ainda coprimos).

O uso da definição para o cálculo do máximo divisor comum de dois números naturais pode ser bastante desconfortável. Por exemplo, se quisermos calcular $\text{mdc}(28997, 9211)$, temos que realizar muitos cálculos até verificar que $\mathcal{D}(28997) = \{1, 107, 271, 28997\}$ e $\mathcal{D}(9211) = \{1, 61, 151, 9211\}$, e concluir que são relativamente primos.

Os antigos matemáticos gregos observaram que o cálculo do máximo divisor comum de dois números naturais pode ser drasticamente simplificado mediante o uso da divisão. De fato, dados números naturais $a$ e $b \neq 0$, sabemos que existem números naturais $q$ e $r$ tais que $a = bq + r$. Dessa identidade percebemos que os divisores comuns a $a$ e a $b$ também são divisores de $r$. Mais exatamente temos o

**Teorema 5.15** (Euclides)**.** *Se $a$, $b$, $q$ e $r$ são números naturais tais que $a = bq + r$, então* $\text{mdc}(a, b) = \text{mdc}(b, r)$.

*Demonstração.* Se $b = 0$ temos $a = r$ e $\text{mdc}(a, b) = a = r = \text{mdc}(b, r)$. Suponhamos $b \neq 0$. Todo divisor comum de $a$ e $b$ também é divisor da combinação linear $a - bq$, portanto de $r$. Em outros termos, todo divisor comum de $a$ e $b$ é divisor comum de $b$ e $r$. Por outro lado, todo divisor comum de $b$ e $r$ é divisor da combinação linear $bq + r$, portanto é divisor de $a$. Em outros termos, todo divisor comum de $b$ e $r$ também o é de $a$ e $b$. Isso quer dizer que $\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(b) \cap \mathcal{D}(r)$. Em consequência esses conjuntos têm o mesmo máximo. Fica assim demonstrado que $\text{mdc}(a, b) = \text{mdc}(b, r)$. □

**Escólio 5.16.** *Se $a$, $b$, $q$ e $r$ são números naturais tais que $a = bq + r$, então os divisores comuns de $a$ e $b$ são também os divisores comuns de $b$ e $r$.*

*Demonstração.* A demonstração do Escólio está contida na demonstração do Teorema 5.15. □

**Escólio 5.17.** *Se $b$, $q$ e $r$ são números naturais então* $\text{mdc}(bq + r, b) = \text{mdc}(b, r)$.

*Demonstração.* Esse escólio é apenas outra maneira de escrever o enunciado do Teorema 5.15. □

O resultado desse Teorema pode ser utilizado para construir um algoritmo que permite calcular o máximo divisor comum de dois números naturais com relativa facilidade. Esse algoritmo é conhecido há muito tempo, e está descrito em *Os Elementos*, de Euclides. Por isso foi denominado *algoritmo euclidiano* pela posteridade.

A ideia surge quando observamos que, dados números naturais $a$ e $b \neq 0$, existem números naturais $q$ e $r$ tais que $a = bq + r$ e $0 \leq r < b$, e o Teorema acima garante que $\text{mdc}(a, b) = \text{mdc}(b, r)$. Assim sendo aparentemente compensa calcular $\text{mdc}(b, r)$ em vez de $\text{mdc}(a, b)$, já que $r < b$. Uma ideia melhor ainda é dividir $b$ por $r$ e novamente diminuir os valores dos números. Assim, se $b = q_1 r + s$, com $0 \leq s < r$, temos $\text{mdc}(b, r) = \text{mdc}(r, s)$. Prosseguindo obtemos uma sequência $0 \leq \ldots < u < t < s < r$, que, após uma quantidade finita de passos, atinge o valor zero. Se $v$ é o último resto não nulo temos $\text{mdc}(a, b) = \text{mdc}(v, 0) = v$.

Dessa forma, sem nenhum esfoço além de o de efetuar divisões, calculamos o máximo divisor comum de dois números naturais quaisquer. Evitamos assim calcular os divisores dos números, o que em geral exige um esforço muito maior.

**Problema resolvido 5.18.** Calcule $\text{mdc}(1365, 231)$ usando o algoritmo euclidiano.

*Solução.* Efetuamos as divisões sucessivas:

$$\begin{aligned} 1365 &= 5 \times 231 + 210, \\ 231 &= 1 \times 210 + 21, \\ 210 &= 10 \times 21 + 0. \end{aligned}$$

Vemos que o último resto não nulo é 21, portanto $\text{mdc}(1365, 231) = 21$. Podemos escrever também:

$$\text{mdc}(1365, 231) = \text{mdc}(231, 210) = \text{mdc}(210, 21) = \text{mdc}(21, 0) = 21.$$

□

Bastante útil na Teoria dos Números é o conceito de mínimo múltiplo comum. Começamos lembrando que, dado um número natural $a$, seus múltiplos são os números $0 \cdot a$, $1 \cdot a$, $2 \cdot a$, ...,

em geral, $n \cdot a$ para todo número natural $n$. Se $a, n \geq 1$ o múltiplo $n \cdot a$ se diz múltiplo positivo. Note que zero só tem um múltiplo, que é ele mesmo. Assim zero não tem múltiplos positivos.

Dado um número natural $a \neq 0$, indicamos por $\mathcal{M}(a)$ o conjunto dos múltiplos positivos de $a$. Por exemplo, $\mathcal{M}(3) = \{3, 6, 9, 12, \ldots\}$.

Notemos que, dados números naturais $a \neq 0$ e $b \neq 0$, o número $ab$ é um múltiplo comum, assim como $2ab$, $3ab$, .... Dessa forma o conjunto $\mathcal{M}(a) \cap \mathcal{M}(b)$ nunca é vazio.

**Definição 5.19.** Dados números naturais $a \neq 0$ e $b \neq 0$, o elemento mínimo do conjunto $\mathcal{M}(a) \cap \mathcal{M}(b)$ chama-se *mínimo múltiplo comum* de $a$ e $b$, e é indicado por $\text{mmc}(a, b)$. Se $a = 0$ ou $b = 0$ convém definir $\text{mmc}(a, b) = 0$.

Por exemplo, $\mathcal{M}(6) \cap \mathcal{M}(9) = \{18, 36, 54, \ldots\}$, portanto $\text{mmc}(6, 9) = 18$.

O estudante está convidado nos Problemas 5.11.19 a 5.11.22 abaixo a detalhar propriedades do mmc.

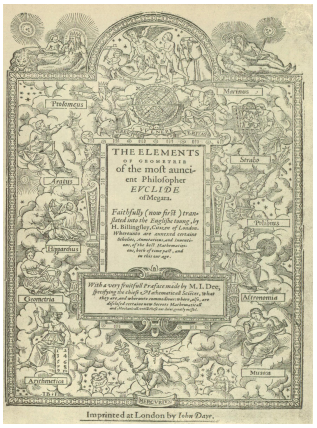



Figura 5.4. Digitalização da capa da primeira edição de Sir Henry Billingsley, em língua inglesa, de *Os Elementos* de Euclides de Alexandria, datada de 1570. Euclides escreveu esse tratado de Matemática por volta de 300 a.C. Os tomos de VII a IX abordam a Teoria dos Números. Euclides define número primo e demonstra, entre outros resultados, que são infinitos. Define o mdc e o mmc e descreve o método que hoje denominamos algoritmo euclidiano para o cálculo do mdc.

## 5.11 Problemas

**Problema 5.11.1.** Cacule $\text{mdc}(54, 66)$ usando a definição de mdc:

$\mathcal{D}(54) = \{$ _____

$\mathcal{D}(66) = \{$ _____

$\mathcal{D}(54) \cap \mathcal{D}(66) = \{$ _____

Resposta: $\text{mdc}(54, 66) =$ _____

**Problema 5.11.2.** Calcule e justifique brevemente:

(i) $\text{mdc}(13245, 5) =$ _____

(ii) $\text{mdc}(17, 3) =$ _____

(iii) para todo número natural $a$ se tem $\text{mdc}(a, 1) =$ _____

(iv) dados $m$ e $n$ números naturais, se tem $\text{mdc}(n, mn) =$ _____

(v) para todo número natural $n$ se tem $\text{mdc}(n, n + 1) =$ _____

(vi) para todo número natural $n$ ímpar se tem $\text{mdc}(n, n + 2) =$ _____

(vii) para todo número natural $n$ par se tem $\text{mdc}(n, n + 2) =$ _____

**Problema 5.11.3.** Cacule $\text{mmc}(21, 35)$ usando a definição de mmc:

$\mathcal{M}(21) = \{$ _____

$\mathcal{M}(35) = \{$ _____

$\mathcal{M}(21) \cap \mathcal{M}(35) = \{$ _____

Resposta: $\text{mmc}(21, 35) =$ _____

**Problema 5.11.4.** Calcule mentalmente:

(i) $\text{mmc}(13245, 5) =$ _____

(ii) $\text{mmc}(17, 3) =$ _____

(iii) para todo número natural $a > 0$ tem-se $\text{mmc}(a, 1) =$ ____

(iv) dados $m > 0$ e $> 0$ números naturais, tem-se $\text{mmc}(n, mn) =$ _

**Problema 5.11.5.** Calcule $\text{mdc}(n, 2n + 1)$ para todo número natural $n$.

**Problema 5.11.6.** Ache $\text{mdc}(12k + 10, 3k + 2)$ para todo número natural $k$.

**Problema 5.11.7.** Explique por que se $p$ e $q$ são primos diferentes então são relativamente primos.

**Problema 5.11.8.** Explique por que se o primo $p$ não é divisor do número natural $b > 1$ então $p$ e $b$ são relativamente primos.

**Problema 5.11.9.** Justifique por que se os números naturais $a$ e $b$ não são relativamente primos então existe um primo $p$ que é divisor comum de ambos.

**Problema 5.11.10.** Justifique por que se $p$ é primo então para todo número natural $a$ se tem $\text{mdc}(p, a) = 1$ ou $\text{mdc}(p, a) = p$. Conclua que ou $a$ e $p$ são relativamente primos ou $a$ é múltiplo de $p$.

**Problema 5.11.11.** Explique por que o número natural $p > 1$ é primo se e somente se para todo número natural $a$ se tem $\text{mdc}(p, a) = 1$ ou $p$ é divisor de $a$.

**Problema 5.11.12.** Justifique por que os números naturais $a \geq 2$ e $b \geq 2$ não têm primo em comum em sua decomposição em fatores primos se e somente se eles são relativamente primos.

**Problema 5.11.13.** Justifique por que se os números naturais $a$ e $b$ são relativamente primos e se $a_1$ e $b_1$ são divisores respectivamente de $a$ e $b$ então $a_1$ e $b_1$ são relativamente primos.

**Problema 5.11.14.** Calcule $\text{mdc}(32277, 14973)$ usando o algoritmo euclidiano.

**Problema 5.11.15.** Calcule $\text{mdc}(123469, 2849)$ utilizando: **a)** o algoritmo euclidiano; **b)** diretamente através da definição de máximo divisor comum. Compare o esforço de cálculo de um método em relação ao outro.

**Problema 5.11.16.** Vimos que $\mathcal{D}(12) \cap \mathcal{D}(18) = \{1, 2, 3, 6\}$ e $\text{mdc}(12, 18) = 6$. Examinando os divisores comuns de 12 e 18, qual sua relação com o máximo divisor comum? Examine outros exemplos. Escreva uma conjectura geral. Alguma demonstração?

**Problema 5.11.17.** Usando a ideia do Problema 5.11.16 verifique que

$$\text{mdc}(a_1, a_2, \ldots, a_n) = \text{mdc}(a_1, a_2, \ldots, a_{n-2}, \text{mdc}(a_{n-1}, a_n))$$

quaisquer que sejam os números naturais $a_1$, $a_2$, ..., $a_n$. Mostre como se pode utilizar recursivamente o algoritmo euclidiano para calcular o máximo divisor comum de $n \geq 3$ números naturais. Aplique a ideia para calcular $\text{mdc}(11571, 1729, 637)$.

**Problema 5.11.18.** Dê exemplos de números naturais $a$, $b$ e $c$ relativamente primos mas que não são relativamente primos quando tomados dois a dois.

**Problema 5.11.19.** Examinando exemplos variados de conjuntos $\mathcal{M}(a) \cap \mathcal{M}(b)$, liste e justifique propriedades do mmc.

**Problema 5.11.20.** Você deve ter percebido, examinando vários exemplos, que se $p$ e $q$ são primos diferentes, parece que vale que $\text{mmc}(p, q) = pq$. Tente uma demonstração geral usando recursos algébricos. Identifique algum resultado que você precisa para demonstrar isso.

**Problema 5.11.21.** Examinando exemplos variados de $\text{mdc}(a, b)$ e $\text{mmc}(a, b)$ conjuntamente, obtenha uma propriedade que os relacione em uma mesma fórmula. Alguma demonstração?

**Problema 5.11.22.** Defina mmc de três ou mais números naturais e mostre que sua definição é consistente.

## 5.12 Algumas identidades algébricas importantes

Vejamos algumas identidades importantes para investigar números primos e compostos. Mas antes estudemos um exemplo simples de uso de uma identidade algébrica nesse contexto.

**Problema resolvido 5.20.** Investigar para quais números naturais a diferença de seus quadrados é primo.

*Solução.* Queremos descobrir todos os números naturais $a$ e $b$ tais que $b^2 - a^2$ seja primo. O estudante pode calcular alguns casos se isso lhe deixar mais seguro na compreensão do enunciado. Em particular, pode obter exemplos em que essa expressão resulta número primo, e exemplos em que resulta número composto. Portanto precisamos descobrir alguma condição sobre $a$ e $b$ que distinga esses dois casos.

Observamos de imediato que não queremos que $b^2 - a^2$ seja negativo e nem zero, de modo que impomos logo a condição $b > a$. Se $a = 0$ então $b^2 - a^2 = b^2$ nunca é primo (por quê?) Supomos então que $b > a \geq 1$.

Já que estamos falando de identidades, não há como deixar de lembrar que

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

é uma relação algébrica muito conhecida dos estudantes do Ensino Fundamental. Ela mostra que $b^2 - a^2$ se decompõe em um produto de dois números. Como $b + a \geq 2$, se ocorrer também que $b - a \geq 2$ então já sabemos que $b^2 - a^2$ é composto. Portanto, para que $b^2 - a^2$ seja primo, a única chance é que $b - a = 1$, ou $b = a + 1$. Nesse caso

$$b^2 - a^2 = (a + 1)^2 - a^2 = a^2 + 2a + 1 - a^2 = 2a + 1,$$

de modo que $b^2 - a^2$ é primo se e somente se $b = a + 1$ e $2a + 1 = a + b$ é primo. Exemplo: $a = 3, b = 4 \Rightarrow b^2 - a^2 = 16 - 9 = 7$, que é primo. □

Uma identidade muito usada em Teoria dos Números é:

**Teorema 5.21** (Fórmula do binômio)**.** *Sejam $x$ e $y$ números reais e $n \geq 1$ um número natural. Então*

$$(x+y)^n = x^n + \binom{n}{1}x^{n-1}y + \binom{n}{2}x^{n-2}y^2 + \ldots + \binom{n}{n-1}xy^{n-1} + y^n. \tag{5.1}$$

Essa relação é conhecida também sob o nome de "fórmula do binômio de Newton", referindo-se ao físico e matemático Isaac Newton.

Os números $\binom{n}{i}$, chamados *números binomiais*, são definidos por

$$\binom{n}{i} = \frac{n!}{i!(n-i)!} \tag{5.2}$$

quaisquer que sejam os números naturais $0 \leq i \leq n$.

Vemos logo abaixo um exemplo de uso dessa identidade. Outras identidades muito úteis:

Sejam $a$, $b$ e $n \geq 2$ números naturais. Então

$$a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \ldots + ab^{n-2} + b^{n-1}). \tag{5.3}$$

Sejam $a$, $b$ e $n > 0$ números naturais. Então

$$a^{2n+1} + b^{2n+1} = (a+b)(a^{2n} - a^{2n-1}b + \ldots - ab^{2n-1} + b^{2n}) \tag{5.4}$$

e

$$a^{2n} - b^{2n} = (a+b)(a^{2n-1} - a^{2n-2}b + \ldots + ab^{2n-2} - b^{2n-1}). \tag{5.5}$$

Consideramos o Teorema 5.21 conhecido do estudante. De qualquer forma o Problema 10.8.1 traz mais informações. As identidades seguintes podem ser demonstradas diretamente. Basta multiplicar os fatores dos segundos lados das identidades.

Segue um exemplo de aplicação da fórmula binomial (5.1):

**Proposição 5.22** (Critério de divisibilidade por três e por nove)**.** *O número $(a_n a_{n-1} \ldots a_1 a_0)_{\text{dez}}$ é múltiplo de 3 (respectivamente de 9) se e somente se $a_n + a_{n-1} + \ldots + a_1 + a_0$ for múltiplo de 3 (respectivamente de 9).*

*Demonstração.* Para todo número natural $j$ temos

$$\begin{aligned} 10^j &= (9+1)^j \\ &= 9^j + \binom{j}{1}9^{j-1} + \ldots + \binom{j}{j-1}9 + 1 \\ &= 9\left[9^{j-1} + \binom{j}{1}9^{j-2} + \ldots + \binom{j}{j-1}\right] + 1 \\ &= 9q_j + 1 \end{aligned}$$

em que $q_j = 9^{j-1} + \binom{j}{1}9^{j-2} + \ldots + \binom{j}{j-1}$ é um número natural. Portanto

$$\begin{aligned}(a_n a_{n-1} \ldots a_1 a_0)_{\text{dez}} &= (9q_n + 1)a_n + (9q_{n-1} + 1)a_{n-1} + \ldots + (9 + 1)a_1 + a_0 \\ &= 9q + a_n + a_{n-1} + \ldots + a_1 + a_0\end{aligned}$$

para um certo número natural $q$. Portanto $(a_n a_{n-1} \ldots a_1 a_0)_{\text{dez}}$ é múltiplo de 3 (respectivamente de 9) se e somente se $a_n + a_{n-1} + \ldots + a_1 + a_0$ for múltiplo de 3 (respectivamente de 9). □

**Problema resolvido 5.23.** Entre 18 números naturais consecutivos quaisquer com três dígitos sempre existe pelo menos um que é múltiplo da soma de seus dígitos.

*Solução.* O estudante, se achar necessário, pode considerar alguns casos e verificar que efetivamente ocorre essa propriedade. Pode também decidir examinar todos os casos possíveis, pois existe uma quantidade finita deles.

Outra opção é partir logo para o uso de relações algébricas. Queremos um número $n = (abc)_{dez}$ de três dígitos tal que

$$n = q(a + b + c) \iff 100a + 10b + c = q(a + b + c)$$

para algum $q$. Manipulando essa relação de todas as formas quase nada conseguimos. E o que interessa o fato de que esse número está em uma lista de 18 consecutivos? Qualquer número está!

Vemos que precisamos de outra estratégia. Procuremos fatos relacionados que já conhecemos de modo que possamos estabelecer alguma analogia. Lembramos dos seguintes:

*1º fato:* a soma dos dígitos de um número apareceu na Proposição 5.22 logo acima: um número é múltiplo de 3 ou de 9 se e somente se a soma de seus dígitos for múltiplo de 3 ou de 9, respectivamente.

Ainda não sabemos se vamos usar isso ou não, mas chama a atenção que 3 e 9 são divisores de 18.

Por outro lado, já vimos alguma propriedade sobre números consecutivos: foi visto no Problema Resolvido 4.16 que "dados três números naturais consecutivos quaisquer, exatamente um deles é múltiplo de 3". Usando analogia temos

*2º fato:* Dados 18 números naturais consecutivos quaisquer, exatamente um deles é múltiplo de 18.

O estudante pode demonstrar esse fato imitando o argumento usado em 4.16. Mas, para se convencer, não é preciso escrever muito: dados 18 números consecutivos, os dividimos um a um por 18, em ordem. Obtemos um a um os dezoito restos possíveis 0, 1, 2, ..., 17 em ordem cíclica, não necessariamente começando por zero, mas certamente o zero será obtido em algum momento. E aí temos um número múltiplo de 18.

Seja $n = (abc)_{dez}$ esse número. Sendo $n$ múltiplo de 18, também é múltiplo de 9. Em virtude do fato 1 elencado acima, $a + b + c$ é múltiplo de 9.

Agora precisamos estar atentos e observar que não existem muitas opções para $a + b + c$. Primeiro notemos que $a$, $b$ e $c$ são algarismos, com $1 \leq a \leq 9$ e $0 \leq b, c \leq 9$. Portanto $1 \leq a+b+c \leq 27$. Ainda, como deve ser múltiplo de 9, só temos as possibilidades $a+b+c = 9$, 18 ou 27. Se $a + b + c = 27$ então $n = 999$, que não é múltiplo de 18, e assim o descartamos. Logo $a+b+c = 9$ ou 18, de modo que $a+b+c$ divide 18, que divide $n$, e assim $a+b+c$ divide $n$. Terminamos. □

**Problema resolvido 5.24.** Demonstre que, para todo número natural $m \geq 2$, se $2^m - 1$ é primo então $m$ é primo.

*Solução.* Seja $m = rs$ uma decomposição qualquer de $m$ como produto de números naturais. Queremos mostrar que, se $2^m - 1$ é primo, necessariamente se tem $r = 1$ ou $s = 1$. Começamos observando que

$$2^m - 1 = 2^{rs} - 1 = (2^r)^s - 1.$$

Usando a identidade 5.3 com $a = 2^r$, $b = 1$ e $n = s$ temos

$$2^m - 1 = (2^r)^s - 1 = (2^r - 1)((2^r)^{s-1} + (2^r)^{s-2} + \ldots + 1).$$

Como $2^m - 1$ é primo, segue que $2^r - 1 = 1$ ou $(2^r)^{s-1} + (2^r)^{s-2} + \ldots + 1 = 1$. Portanto $r = 1$ ou $s = 1$, respectivamente. Provamos que $m$ é primo. □

## 5.13 Problemas

**Problema 5.13.1. a)** Explique por que para todo número natural $n$ se tem $10^n = 11q_n + (-1)^n$ para algum número natural $q_n$. **b)** Justifique por que um número natural $(a_n a_{n-1} \ldots a_1 a_0)_{dez}$ é múltiplo de 11 se e somente se $a_0 - a_1 + a_2 - a_3 + \ldots + (-1)^n a_n$ for múltiplo de 11. Teste esse método em alguns exemplos.

**Problema 5.13.2.** Investigue para quais números naturais $n$ o número $6^n - 1$ é primo.

**Problema 5.13.3. a)** Demonstre que $10^{2n} - 1$ é múltiplo de 11 para todo número natural $n$. **b)** Prove que $10^{2n+1} + 1$ é múltiplo de 11 para todo número natural $n$.

**Problema 5.13.4.** Caracterize os múltiplos de 11 de um só algarismo.

**Problema 5.13.5.** Determine todos os números naturais $n$ para os quais $n^3 + 1$ é primo.

**Problema 5.13.6.** Determine todos os números naturais $n$ para os quais $8^n + 1$ é composto.

**Problema 5.13.7.** Prove que a diferença entre um número natural e a soma dos dígitos de sua representação decimal é múltiplo de 9.

**Problema 5.13.8.** Veja se existem versões da Proposição 5.22 e do Problema 5.13.7 para números representados em uma base $\beta$ qualquer.

**Problema 5.13.9.** Encontre o resto da divisão de $1 + 4^n$ por 3 para todo número natural $n$.

**Problema 5.13.10.** Sabendo-se que $a^n - 1$ é primo, o que se pode dizer sobre os números naturais $a$ e $n$?

**Problema 5.13.11.** Com o auxílio do Teorema 5.21 demonstre que $m^n$ e $m$ têm a mesma paridade, quaisquer que sejam os números naturais $m \geq 0$ e $n \geq 1$.

**Problema 5.13.12.** Encontre todos os números primos que se escrevem como soma de dois cubos (não necessariamente diferentes).

**Problema 5.13.13.** Encontre todos os números primos que se escrevem como soma de duas potências quínticas (não necessariamente diferentes).

## 5.14 Comentários adicionais

No capítulo anterior vimos como a Escola Pitagórica deu início à Teoria dos Números, e como suas investigações trouxeram inúmeras perguntas, e citamos algumas delas:

1. A quantidade de números primos é finita ou infinita?
2. Como testar a primaridade de um número?
3. Como produzir uma lista de números primos da forma mais rápida e cômoda possível?
4. Dado um número composto, como encontrar seus fatores?
5. A decomposição de um número natural $n \geq 2$ como produto de fatores primos é única?
6. A sequência dos números primos tem uma regra de formação que possa facilitar sua obtenção? Existe uma fórmula adequada que forneça o $n$-ésimo número primo?

Neste capítulo trabalhamos com as quatro primeiras questões. Demonstramos que existem infinitos números primos. Vimos que para verificar a primaridade de um número natural $n > 2$ basta dividi-lo por todos os primos $\leq \sqrt{n}$. Estudamos o método do crivo, que permite listar números primos e encontrar uma decomposição de um número composto como produto de primos.

Devemos observar entretanto que os métodos de crivagem são considerados lentos, mesmo quando implementados em computadores digitais. Devido a isso a Teoria dos Números desenvolveu, e continua desenvolvendo, novos métodos que permitem testar a primaridade de números ou obter uma decomposição em fatores primos através de algoritmos mais rápidos. O estudante pode ler mais informações em [102].

No Capítulo 7 respondemos à questão do item 5. O Teorema Fundamental da Aritmética estabelece que a decomposição de um número natural $n \geq 2$ como produto de fatores primos é única.

Quanto à última questão observamos que ela constitui o chamado problema da distribuição dos números primos, e tem grande importância na Teoria dos Números. Entretanto não iremos abordá-la neste livro introdutório. O estudante deverá procurar outros livros de Teoria dos Números para se informar mais.

Finalmente observamos que o aparecimento dos sistemas computacionais algébricos trouxe grande facilidade no estudo dos números. Esses sistemas proporcionam economia de tempo e esforço, e permitem realizar cálculos antes impensáveis. Por isso sugerimos ao estudante aprender a utilizar esses sistemas. A situação ideal é aquela em que o estudante de Teoria dos Números sempre tenha um desses sistemas à mão de modo a facilitar a realização de experimentos numéricos e algébricos que acompanhem o estudo teórico dos conceitos e técnicas.

## 5.15 Problemas adicionais

**Problema 5.15.1.** Não se sabe o valor dos dígitos $a$ e $b$ de $(7272ab)_{dez}$, mas se sabe que esse número é múltiplo de 99. Verifique se com essa informação é possível determinar os valores dos dois dígitos desconhecidos.

**Problema 5.15.2.** Verifique se é possível que num triângulo as medidas em graus dos ângulos internos possam ser todas números primos. Em caso positivo dê todas as possibilidades.

**Problema 5.15.3.** Um estudante escreveu em cada face de um cubo um número natural positivo. Em seguida escreveu em cada vértice o produto dos números escritos nas faces que se encontram nesse vértice. Se a soma dos números escritos nos vértices é 105, qual é a soma dos números escritos nas faces?

**Problema 5.15.4.** Prove que $p > 1$ é primo se e somente se $\text{mdc}(a, p) = 1$ para todo número natural $a$ tal que $1 \leq a \leq \sqrt{p}$.

**Problema 5.15.5.** Mostre que funciona corretamente o seguinte procedimento para verificar se um dado número natural $p \geq 4$ é ou não primo. Indicamos por $[\sqrt{n}\,]$ a parte inteira de $\sqrt{n}$. Dado $p$, reserve o valor de $[\sqrt{p}\,]$.

Dado um número natural $a$, chamamos de $(C)$ o seguinte comando:

$$(C) \quad \text{calcule } \text{mdc}(a, p) = d.$$

*Instruções*: comece com $a = 2$ e execute $(C)$. Se $d > 1$ pare e guarde o valor de $a$. Se $d = 1$ tome como $a$ o seu sucessor. Se $a > [\sqrt{p}\,]$ pare e guarde o valor de $a$. Se $a \leq [\sqrt{p}\,]$ execute novamente $(C)$ e as instruções seguintes.

Ao terminar o procedimento, se $a \leq [\sqrt{p}\,]$, então $p$ é composto, e se $a > [\sqrt{p}\,]$ então $p$ é primo.

**Problema 5.15.6.** Verifique que, se $n \geq 2$ é um número natural, escolhendo-se $n + 1$ números quaisquer dentre 1, 2, 3, ..., $2n$, pelo menos dois dos escolhidos são relativamente primos.

**Problema 5.15.7.** Seja $p \geq 5$ um número primo. Mostre que 1 é o resto da divisão de $p^2$ por 24. Qual é um enunciado mais geral dessa afirmação?

**Problema 5.15.8.** Estude o seguinte método para o cálculo do mdc e do mmc, e entenda por que ele funciona. Exemplificamos com 2100 e 198. Primeiro decompomos em primos os números dados usando a seguinte disposição:

| | | | |
|---|---|---|---|
| 2100 | 2 | 198 | 2 |
| 1050 | 2 | 99 | 3 |
| 525 | 3 | 33 | 3 |
| 175 | 5 | 11 | 11 |
| 35 | 5 | 1 | |
| 7 | 7 | | |
| 1 | | | |

Em seguida coletamos os divisores primos da seguinte forma. Para o mdc tomamos apenas os divisores primos comuns e com a menor multiplicidade com que aparecem em ambas as decomposições. Dessa forma $\text{mdc}(2100, 198) = 2 \cdot 3 = 6$. Para o mmc tomamos todos os divisores primos, comuns e não comuns, e com a maior multiplicidade. Dessa forma $\text{mmc}(2100, 198) = 2^2 \cdot 3^2 \cdot 5^2 \cdot 7 \cdot 11 = 69300$.

Use esse método para calcular $\text{mdc}(84, 90)$ e $\text{mmc}(84, 90)$. Faça o mesmo com 1001 e 4235.

A justificativa desse método está apresentada formalmente no Teorema 7.16. É um dispositivo que costuma ser usado no Ensino Fundamental.

Aplica-se também para o cálculo do mdc e do mmc de três ou mais números. Calcule $\text{mdc}(20, 30, 14)$ e $\text{mmc}(20, 30, 14)$.

**Problema 5.15.9.** Segue uma variante do método descrito no problema anterior. A decomposição é simultânea. Na última coluna comparece um primo sempre que ele for divisor de pelo menos um dos números. Multiplicando todos os primos assim obtidos temos o mmc dos números. Exemplo:

| | | |
|---|---|---|
| 2100 | 198 | 2 |
| 1050 | 99 | 2 |
| 525 | 99 | 3 |
| 175 | 33 | 3 |
| 175 | 11 | 5 |
| 35 | 11 | 5 |
| 7 | 11 | 7 |
| 1 | 11 | 11 |
| 1 | 1 | |

Portanto $\text{mmc}(2100, 198) = 2^2 \cdot 3^2 \cdot 5^2 \cdot 7 \cdot 11 = 69300$.

Calcule $\text{mmc}(84, 90)$ e $\text{mmc}(1001, 4235)$ usando esse método. Justifique esse método comparando-o com o do Problema 5.15.8. Identifique uma forma para que essa variante também forneça o mdc. Essa variante funciona para três ou mais números? Dê um exemplo.

**Problema 5.15.10.** A seguinte variante tem a vantagem de ser mais compacta e de fornecer simultaneamente o mdc e o mmc. Na decomposição simultânea só aparecem os primos que são divisores comuns.

| | | |
|---|---|---|
| 2100 | 198 | 2 |
| 1050 | 99 | 3 |
| 350 | 33 | |

O método permite concluir que $\text{mdc}(2100, 198) = 2 \cdot 3 = 6$ e $\text{mmc}(2100, 198) = 2 \cdot 3 \cdot 350 \cdot 33 = 69300$.

Use esse método para calcular o mdc e o mmc de 84 e 90, e de 1001 e 4235. Justifique esse método comparando-o com o do Problema 5.15.8. Essa variante funciona para três ou mais números? Dê um exemplo.

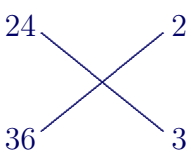
**Problema 5.15.11.** Estude a seguinte variação do dispositivo do Problema 5.15.10:

$$\frac{2100}{198} \overset{2}{=} \frac{1050}{99} \overset{3}{=} \frac{350}{33}$$

$\Rightarrow \text{mdc}(2100, 198) = 2 \cdot 3 = 6$ e $\text{mmc}(2100, 198) = 2 \cdot 3 \cdot 350 \cdot 33 = 69300$.

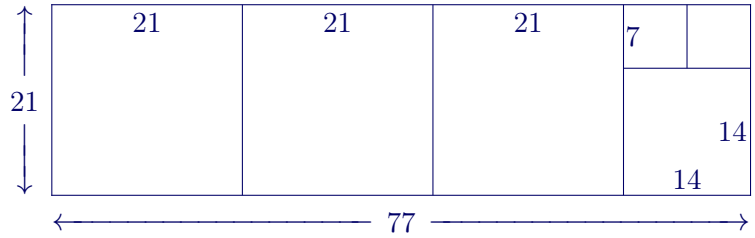
**Problema 5.15.12.** Estude o que ocorre em

$$\begin{array}{lllllll} 24 & = & 2 & 2 & 2 & 3 & \\ 36 & = & 2 & 2 & & 3 & 3 \end{array}$$



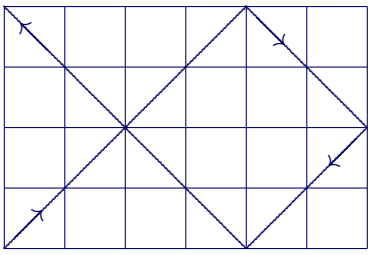

$\Rightarrow \text{mmc}(24, 36) = 24 \times 3 = 72$ ou $\text{mmc}(24, 36) = 36 \times 2 = 72$. Por quê?

**Problema 5.15.13.** Estude e justifique o seguinte método geométrico de calcular o mdc. Sejam $a$ e $b$ números naturais não nulos. Consideremos o retângulo de lados $a$ e $b$. Recobrimos a região retangular com quadrados cujos lados são números naturais, os maiores possíveis, conforme ilustra a figura abaixo em que $a = 77$ e $b = 21$. Então $\text{mdc}(a, b)$ é o lado do menor quadrado. Na figura abaixo o menor quadrado tem lados iguais a 7, portanto $\text{mdc}(77, 21) = 7$.




**Problema 5.15.14.** Estude e justifique o seguinte método geométrico de calcular o mmc. Sejam $a$ e $b$ números naturais não nulos. Consideremos o retângulo de lados $a$ e $b$. Subdividimos o retângulo em $ab$ quadrados unitários. Um raio de luz sai de um dos vértices do retângulo fazendo um ângulo de 45° com os lados. Sempre que atinge um lado do retângulo $a \times b$, o raio é refletido de volta para o seu interior, até que atinja novamente um de seus vértices, quando sai para o exterior. A quantidade de quadrados unitários atravessados pelo raio de luz é o $\text{mmc}(a, b)$.

A figura abaixo ilustra o caso em que $a = 6$ e $b = 4$. O raio de luz atravessou 12 quadrados unitários, portanto $\text{mmc}(6, 4) = 12$.



**Problema 5.15.15.** Dona Leonor é quituteira do bairro, e certo dia recebeu três encomendas, de 200, 240 e 300 empadinhas, respectivamente. Feitas as empadinhas, dona Leonor as separou em pacotes iguais. Quantas empadas foram colocadas em cada pacote, sabendo-se que foram feitos o menor número possível de pacotes, e que cada freguês recebeu exatamente a quantia encomendada? Quantos pacotes recebeu cada freguês?

**Problema 5.15.16.** Pedrinho toma um remédio de 10 em 10 dias e outro de 15 em 15 dias. Sua mãe assinala os dias em um calendário, marcando com um círculo o dia em que é tomado o primeiro remédio, e com um quadradinho o dia em que é tomado o segundo remédio. No dia 17 de janeiro de 2010 os dois dias coincidiram em um domingo. Quando essa coincidência voltou a acontecer novamente pela primeira vez?

**Problema 5.15.17.** Um terreno retangular tem 1575 metros de comprimento e 440 de largura. O proprietário deseja cercar o terreno com uma cerca de arame apoiada em mourões. Ele quer que ao longo de todo o perímetro a distância entre dois mourões consecutivos seja constante. Calcule a maior distância possível. Quais são outras soluções para o problema? Qual a melhor solução considerando o contexto?

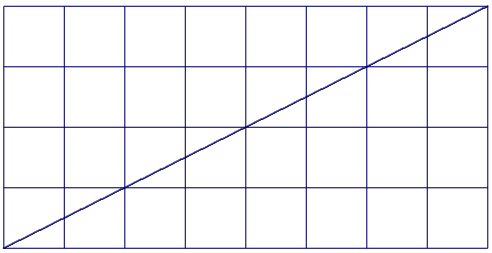
**Problema 5.15.18.** Duas rodas de uma engrenagem têm 45 e 60 dentes, respectivamente. Cada roda tem exatamente um dente quebrado. Se, num dado instante, os dentes quebrados

estão em contato, depois de quantas voltas da roda maior eles estarão novamente em contato pela primeira vez? Quantas voltas terá dado a roda menor?

**Problema 5.15.19.** Um planeta e as órbitas de suas três luas estão contidas em um plano. Os períodos de translação das luas são 60, 84 e 132 unidades de tempo. Se num determinado instante as luas estão alinhadas com o planeta em uma determinada direção, quando isso acontecerá novamente pela primeira vez? Quantas translações terá executado cada uma das luas?

**Problema 5.15.20.** Numa República o Presidente permanece no cargo por 6 anos, os senadores por 8 e os governadores por 4. Se num determinado ano houve novos mandatos simultâneos para os três cargos, quando isso acontecerá novamente pela primeira vez?

**Problema 5.15.21.** Sejam $m$ e $n$ números naturais positivos. Considere um retângulo cujos lados medem $m$ e $n$ unidades. Traçando retas paralelas aos lados do retângulo, divida seu interior em $mn$ quadrados unitários. Calcule quantos quadrados unitários têm seu interior interceptados por uma diagonal do retângulo.



**Problema 5.15.22.** Seja $n$ um número natural. **a)** Mostre que existe um número natural $t$ tal que $n < 3^t$. **b)** Explique por que $n$ pode ser escrito na forma $n = 3^j b$ para algum número natural $j$ e para algum número natural $b$ que não é múltiplo de 3.

**Problema 5.15.23.** Demonstre que os únicos primos divisores de $n = 2^i 3^j$, $1 \leq i, j$, são 2 e 3.

## 5.16 Temas para investigação

**Tema 5.16.1.** Investigue para quais números naturais $m$ vale a seguinte afirmação: "se $m$ é divisor do produto $ab$ então $m$ é divisor de $a$ ou de $b$, quaisquer que sejam os números naturais $a$ e $b$."

**Tema 5.16.2.** Um estudante conjecturou que a diferença de dois números naturais cúbicos consecutivos quaisquer é primo. Imagine o que teria levado o estudante fazer essa conjectura. Verifique a conjectura. Pesquise o que ocorre com outras potências.

**Tema 5.16.3.** Um estudante, para verificar se 79 é primo, pensou o seguinte: 79 não é múltiplo de 7 e dividido por 30 resta 19; como $19 > 5$ é primo, então 79 é primo. Faça um detalhamento desse método. Crie um teste de primaridade para números $2 \leq n \leq 120$. Explique tudo.

**Tema 5.16.4.** Você pode decompor 8051 em produto de dois números usando apenas cálculo mental. Os dois fatores são primos? (use o problema anterior para decidir isso).

**Tema 5.16.5.** Investigue a primaridade das rep-unidades $1_n = 11\ldots1$, em que a quantidade de 1's é $n$. Por exemplo, será que $1_n$ é primo se e somente se $n$ é primo? Quais as condições necessárias e suficientes para que $1_n$ seja divisor de $1_m$? Como são os divisores de $1_m$? O que dá $1_m \times 1_n$? O que é $\text{mdc}(1_m, 1_n)$? O que são as rep-unidades na base nove?

**Tema 5.16.6.** Estude os eventos abaixo. Alguma conjectura? Verifique. Alguma generalização?

$f(n) = n^2 - n + 11 \quad f(-1) = 13,\ f(0) = 11,\ f(1) = 11,\ f(2) = 13,\ f(3) = 17$

$f(n) = n^2 - n + 17 \quad f(-1) = 19,\ f(0) = 17,\ f(1) = 17,\ f(2) = 19,\ f(3) = 23$

**Tema 5.16.7.** Considere os seguintes eventos:

$\mathcal{D}(2^1 - 1) = \{1\}$
$\mathcal{D}(2^2 - 1) = \{1, 3\}$
$\mathcal{D}(2^3 - 1) = \{1, 7\}$
$\mathcal{D}(2^4 - 1) = \{1, 3, 5, 15\}$
$\mathcal{D}(2^5 - 1) = \{1, 31\}$
$\mathcal{D}(2^6 - 1) = \{1, 3, 7, 9, 21, 63\}$
$\mathcal{D}(2^7 - 1) = \{1, 127\}$
$\mathcal{D}(2^8 - 1) = \{1, 3, 5, 15, 17, 51, 85, 255\}$
$\mathcal{D}(2^9 - 1) = \{1, 7, 73, 511\}$
$\mathcal{D}(2^{10} - 1) = \{1, 3, 11, 31, 33, 93, 341, 1023\}$
$\mathcal{D}(2^{11} - 1) = \{1, 23, 89, 2047\}$
$\mathcal{D}(2^{12} - 1) = \{1, 3, 5, 7, 9, 13, 15, 21, 35, 39, 45, 63, 65, 91, 105, 117, 195, 273,$
$315, 455, 585, 819, 1365, 4095\}$

**a)** Observe as regularidades. Alguma conjectura? Alguma demonstração?

**b)** Generalize. Calcule os divisores de $n^j - 1$ para outros valores de $n$, como $n = 3$, $n = 4$, etc. Quais das regularidades observadas em a) permanecem? Outras conjecturas? Demonstrações?

**Tema 5.16.8.** Os números da forma $M_p = 2^p - 1$, com $p$ primo, são denominados *números de Mersenne*. No Problema Resolvido 5.24 foi visto que, para todo número natural $m \geq 2$, se $2^m - 1$ é primo então $m$ é primo. Verifique se vale a recíproca dessa afirmação. Em 1640 Mersenne afirmou que $M_p$ é primo para $p = 13$, 17, 19, 31, 67, 127 e 257. Verifique essa afirmação. Obtenha na literatura outras informações sobre os números de Mersenne.

**Tema 5.16.9.** Podemos construir testes de primaridade usando condições suficientes. Por exemplo, considere a afirmação:

$$\text{se } p \geq 2 \text{ divide } (p-1)! + 1 \text{ então } p \text{ é primo.}$$

Teoricamente podemos usar essa afirmação para verificar se um dado número natural é primo. Por exemplo, para ver que 5 é primo basta calcular $(5-1)! + 1 = 25$ e constatar que 5 divide 25.

**a)** Demonstre a afirmação acima.

**b)** Verifique se ela é um teste de primaridade de aplicação mais fácil que o dado na seção 5.4.

**c)** Verifique se o teste pode ser melhorado substituindo-se $(p-1)! + 1$ por $(p-3)! + 1$.

**Tema 5.16.10.** Considere a sequência dos números capicuas (em ordem crescente)

$$a_1 = 1,\ a_2 = 2,\ \ldots,\ a_9 = 9,\ a_{10} = 11, \ldots$$

e a sequência das diferenças dos termos consecutivos

$$b_1 = a_2 - a_1,\ b_2 = a_3 - a_2, \ldots$$

Investigue as propriedades da sequência $(b_n)_{n\geq 1}$.

**Tema 5.16.11.** No Problema resolvido 5.2 foram dados alguns exemplos em que $p^2+8$ é primo. Enuncie a conjectura que esses eventos sugerem. Como você iniciaria uma investigação para decidir sobre a validade dessa conjectura?

**Tema 5.16.12.** Vimos que se $n = x^2 - y^2$ é a diferença de dois quadrados tais que $x > y + 1$, então $n$ é composto, e $x + y$ e $x - y$ são fatores. A recíproca é verdadeira: todo composto é a diferença de dois quadrados (o segundo pode ser nulo). Para comprovar isso verifique a identidade: se $n = ab$ então $n = [(a + b)/2]^2 - [(a - b)/2]^2$. Use essa informação para criar um algoritmo de fatoração. Esse é o método de fatoração de Pierre de Fermat. Para obter mais detalhes confira [24] página 40. Aplique o algoritmo para fatorar $n = 302\,303$. Teste o algoritmo com um algum $n$ primo.

# Capítulo 6

# O algoritmo da divisão e aplicações

## 6.1 Introdução

Nos capítulos anteriores estudamos, através da divisão, diversos aspectos das relações entre dois números naturais quaisquer. No presente capítulo vamos formalizar esse estudo com a demonstração do Teorema do Algoritmo da Divisão. Desenvolvemos também uma importante aplicação, o Teorema da Existência e Unicidade da representação dos números naturais em um sistema posicional qualquer.

## 6.2 O Teorema do Algoritmo da Divisão

Diversas vezes nos referimos ao fato de que, dados números naturais $a$ e $b$, com $b \neq 0$, podemos dividir $a$ por $b$, e obter um quociente $q$ e um resto $r$ tal que $r < b$ e $a = bq + r$. O estudante certamente já está convencido da existência de $q$ e $r$, pois tantas vezes já fez esse tipo de cálculo! De fato, se $b \leq a$, sabemos que podemos reunir as unidades de $a$ em grupos de $b$ unidades, tomando tantos grupos quanto for possível, de modo que restarão $r < b$ unidades. Nesse caso $q$ é a quantidade de grupos de $b$ unidades, e temos $a = bq + r$. Por outro lado, se $a < b$, tomamos $q = 0$ e $r = a$, e temos $a = bq + r$, com $r < b$.

Outra propriedade que admitimos de forma natural é que o quociente e o resto são únicos (com a condição $r < b$). Assim se duas pessoas fazem uma conta de dividir usando o algoritmo usual, e obtêm resultados diferentes, logo pensamos: "pelo menos uma delas errou a conta".

O teorema abaixo estabelece essas propriedades mais formalmente.

**Teorema 6.1.** *Dados números naturais $a$ e $b > 0$, existe e é único o par de números naturais $q$ e $r$ tal que*

$$a = bq + r, \quad \textit{com } r < b.$$

*Demonstração.* Vejamos inicialmente a existência dos números $q$ e $r$. Conforme já observamos, se $a < b$ tomamos $q = 0$ e $r = a$, e temos $a = bq + r$, com $r < b$. Suponhamos $b \leq a$. Fazemos as subtrações sucessivas $a - b$, $a - 2b$, $a - 3b$, etc, enquanto essa diferença for $\geq 0$. Quando isso não ocorrer mais, encontramos $q$ tal que $a - qb \geq 0$ e $a < (q + 1)b$. Seja $r = a - qb$. Como $a - qb \geq 0$, vemos que $r$ é um número natural. Ainda, de $a < (q + 1)b$ vem $a - qb < b \Rightarrow r < b$. Isso estabelece a existência de $q$ e $r$.

Vejamos agora a unicidade. Sejam $q$ e $r$ números naturais tais que $a = bq + r$ e $r < b$, e sejam $p$ e $s$ números naturais tais que $a = bp + s$ e $s < b$. Nosso objetivo é demonstrar que $q = p$ e $r = s$. Sem perda de generalidade podemos supor $p \leq q$. Disso segue $bp \leq bq$. Comparando

aquelas identidades vem $bp + s = bq + r \Rightarrow s = bq - bp + r \Rightarrow s = b(q - p) + r$. Temos $r \leq s$ e $s - r = b(q - p)$. Temos também $s - r \leq s < b$. Se fosse $q > p$, teríamos $q - p \geq 1$ e $s - r = b(q - p) \geq b$, o que seria uma contradição. Segue que $q = p$. De $s - r = b(q - p)$ obtemos $s - r = 0 \Rightarrow r = s$. Fica demonstrada a unicidade do par $q$ e $r$. □

Dados números naturais $a$ e $b \neq 0$, denominamos *divisão euclidiana de $a$ por $b$* a existência dos números naturais $q$ e $r$ tais que $a = bq + r$ e $r < b$. Convencionou-se denominar o Teorema 6.1 acima como *Teorema do Algoritmo da Divisão Euclidiana*, ou simplesmente *Teorema do Algoritmo da Divisão*.

Dados números naturais $a$ e $b \neq 0$, podemos dividir $a$ por $b$ e obter números naturais $q$ e $r$ não necessariamente com $r < b$. Neste caso a divisão não é denominada euclidiana. Por exemplo, dividindo $a = 35$ por $b = 8$, podemos ter $35 = 8 \times 3 + 11$, com $q = 3$ e $r = 11$. Nesse caso $q = 3$ e $r = 11$ constituem um quociente e um resto da divisão de $a = 35$ por $b = 8$. A divisão euclidiana fornece $35 = 8 \times 4 + 3$, com $q = 4$ e $r = 3$. Vemos assim que a unicidade de $q$ e $r$ depende da condição $r < b$.

Conforme já sabemos, um caso especial do Teorema 6.1 ocorre quando $r = 0$, e $a$ é dito ser múltiplo de $b$, ou $b$ é dito ser divisor ou fator de $a$.

**Problema resolvido 6.2.** Encontre todos os números naturais $n \geq 1$ tais que 3 é divisor de $5n - 1$.

*Solução.* Fazendo algumas tentativas vemos que $n$ pode ser 2, 5, 8, e não pode ser 1, 3, 4, 6, 7. Assim parece dar certo para $n$ da forma $3q + 2$, e não dar certo para $n$ da forma $3q$ ou $3q + 1$. De fato, se $n = 3q + 2$ para algum natural $q$, então $5n - 1 = 15q + 9 = 3(5q + 3)$, e $5n - 1$ é múltiplo de 3. Se $n = 3q$ para algum natural $q$ então $5n - 1 = 15q - 1$, e $5n - 1$ não é múltiplo de 3. Se $n = 3q + 1$ para algum natural $q$ então $5n - 1 = 15q + 4$, e $5n - 1$ não é múltiplo de 3. Para finalizar, observamos que, ao dividir $n$ por 3, os restos possíveis são 0, 1 ou 2. Assim, já examinamos todos os casos, e os números procurados são os da forma $n = 3q + 2$. □

**Problema resolvido 6.3.** Demonstre que, dado um número natural $n$, existe um múltiplo de $n$ que se escreve com dígitos 1's seguidos, se necessário, de dígitos 0's.

*Solução.* Consideremos os $n$ números naturais 1, 11, 111, ..., $11\ldots1$ (esse último com $n$ dígitos 1's). Se um deles for múltiplo de $n$, terminamos. Do contrário, ocorre que a divisão de cada um desses números por $n$ deixa um dos restos 1, 2, 3, ..., $n - 1$. Como são $n - 1$ possibilidades para os restos e são $n$ números, necessariamente existem dois dos números 1, 11, 111, ... que divididos por $n$ deixam restos iguais. A diferença do maior para o menor é da forma requerida e é um múltiplo de $n$. Confira também o Problema 6.3.1. □

**Problema resolvido 6.4.** Sejam $n \geq 1$ e $a \geq 1$ números naturais, e seja $q$ o quociente da divisão euclidiana de $n$ por $a$. Mostre que $q$ é a quantidade de múltiplos de $a$ no conjunto $S = \{1, 2, 3, \ldots, n\}$.

*Solução.* Se $n < a$ temos $q = 0$ e nenhum elemento de $S$ é múltiplo de $a$. Portanto o resultado vale nesse caso. Suponhamos $a \leq n$. Seja $s$ a quantidade de elementos de $S$ que são múltiplos de $a$. Esses números são exatamente:

$$a,\ 2a,\ 3a,\ \ldots,\ sa.$$

Como $sa$ pertence a $S$ e $(s + 1)a$ não, temos $sa \leq n < (s + 1)a$. Mas, conforme se viu no Teorema 6.1, $q$ é o único número natural tal que $qa \leq n < (q + 1)a$. Dessa forma $q = s$. □

Para todo número real $x \geq 0$, indicaremos por $\lfloor x \rfloor$ o maior dentre os números naturais $\leq x$. Por exemplo,

$$\lfloor 1,2 \rfloor = 1, \quad \lfloor \pi \rfloor = 3, \quad \lfloor 5/6 \rfloor = 0.$$

**Problema resolvido 6.5.** Sejam $n$ e $a \geq 1$ números naturais, e seja $q$ o quociente da divisão euclidiana de $n$ por $a$. Mostre que $q = \lfloor n/a \rfloor$. Portanto $\lfloor n/a \rfloor$ é a quantidade de múltiplos de $a$ no conjunto $\{1, 2, 3, \ldots, n\}$.

*Solução.* Seja $n = aq + r$, com $0 \leq r < a$. Então

$$\frac{n}{a} = q + \frac{r}{a} \Rightarrow \left\lfloor \frac{n}{a} \right\rfloor = \left\lfloor q + \frac{r}{a} \right\rfloor = q$$

pois $q$ é número natural e $0 \leq r/a < 1$. □

**Problema resolvido 6.6.** Seja $n$ um número natural. Calcule a quantidade de elementos de $\{1, 2, 3, \ldots, n\}$ que são múltiplos de 2 ou de 3.

*Solução.* Um estudante mais apressado poderia dizer que é $\lfloor n/2 \rfloor + \lfloor n/3 \rfloor$, mas nessa soma estaria contando duas vezes os múltiplos de $2 \cdot 3 = 6$. Portanto o número procurado é

$$\left\lfloor \frac{n}{2} \right\rfloor + \left\lfloor \frac{n}{3} \right\rfloor - \left\lfloor \frac{n}{6} \right\rfloor.$$

□

## 6.3 Problemas

**Problema 6.3.1.** Mostre que se os números naturais $a \geq b$ têm um mesmo resto quando divididos por $c$, então a diferença $a - b$ é um múltiplo de $c$.

**Problema 6.3.2.** Demonstre que, para todo número natural $a$, o dígito das unidades da representação decimal de $a$ é exatamente o resto da divisão de $a$ por 10.

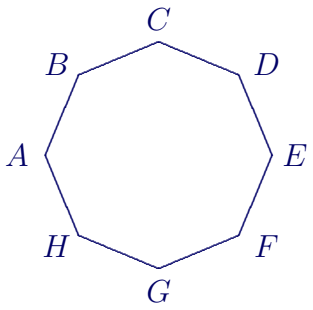
**Problema 6.3.3.** Observando o dígito da unidade da representação decimal de um número natural, em que situações é possível garantir que o número não é um quadrado perfeito?

**Problema 6.3.4.** Demonstre que a soma dos quadrados de dois números ímpares não é um quadrado perfeito.

**Problema 6.3.5.** Encontre a 2010ª. letra da sequência periódica

XWDTURYXWDTURYXWDTURYXWDTURYXWDT ...

**Problema 6.3.6.** Os pontos $A$, $B$, $C$, $D$, $E$, $F$, $G$ e $H$ são vértices consecutivos de um octógono regular. A partir de $A$, no sentido horário de rotação, associamos a esses pontos ordenadamente os números naturais 1, 2, 3, ..., de modo que $A \to 1$, $B \to 2$, $C \to 3$, $D \to 4$, $E \to 5$, $F \to 6$, $G \to 7$, $H \to 8$, $A \to 9$, $B \to 10$, e assim por diante. Calcule a que letra está associado o número 2008.




**Problema 6.3.7.** Seja $n$ um número natural qualquer. Demonstre que se 11 divide $10n$, então 11 divide $n$.

**Problema 6.3.8.** Prove detalhadamente que $(a_n \dots a_1 a_0)_{dez}$ é múltiplo de 11 se e somente se $(a_n \dots a_1)_{dez} - a_0$ também o for. Use esse resultado para verificar que 7 153 474 108 é múltiplo de 11.

**Problema 6.3.9. a)** Verifique se existem primos $p$ tais que $p+4$, $p+6$ e $p+8$ também são primos. **b)** Faça o mesmo com $p$, $p+2$, $p+4$ e $p+6$.

**Problema 6.3.10. a)** Encontre todos os números naturais $n$ para os quais 5 é divisor de $3n+1$. **b)** Encontre todos os números naturais $n$ para os quais 6 é divisor de $3n+1$.

## 6.4 Existência e unicidade em sistemas posicionais

No Capítulo 2, seção 2.6, vimos o que são sistemas posicionais de base $\beta$ para um número natural $\beta \geq 2$ qualquer, e que todo número natural tem representação nesse sistema. O teorema abaixo formaliza essa afirmação e estabelece a unicidade da representação.

**Teorema 6.7.** *Seja $\beta \geq 2$ um número natural. Todo número natural $n \geq 1$ pode ser escrito de maneira única na forma*

$$n = d_t\beta^t + d_{t-1}\beta^{t-1} + \cdots + d_1\beta + d_0 \tag{6.1}$$

*para algum $t \geq 0$ e os números $d_i$ são tais que $d_t \neq 0$ e $0 \leq d_i < \beta$ para $i = 0, 1, 2, \dots, t$.*

A representação 6.1, conforme já sabemos, denomina-se *representação de $n$ na base $\beta$*. Os números $d_j$ são chamados *dígitos* de $n$ na base $\beta$. A unicidade da representação significa que se

$$d_t\beta^t + d_{t-1}\beta^{t-1} + \cdots + d_1\beta + d_0 = f_s\beta^s + f_{s-1}\beta^{s-1} + \cdots + f_1\beta + f_0,$$

com $f_s \neq 0$ e $0 \leq f_i < \beta$ para $i = 0, 1, 2, \dots, s$, então $t = s$ e $d_i = f_i$ para todo $i$.

A representação 6.1 pode ser escrita na forma compacta

$$(d_t d_{t-1} \dots d_1 d_0)_\beta \tag{6.2}$$

e, se estiver claro de que base se trata, escrevemos apenas $d_t d_{t-1} \dots d_1 d_0$.

*Demonstração do Teorema 6.7*

As potências $\beta^0$, $\beta^1$, $\beta^2$, $\beta^3, \ldots, \beta^i, \ldots$ formam uma sequência estritamente crescente de números naturais. Então $n$ coincide com uma dessas potências ou está entre duas consecutivas. Seja $t$ o (único) número natural tal que

$$\beta^t \leq n < \beta^{t+1}.$$

Dividindo $n$ por $\beta^t$ encontramos um quociente $d_t$ e um resto $r_t$ tais que

$$n = d_t\beta^t + r_t \quad \text{e} \quad r_t < \beta^t.$$

Como $\beta^t \leq n$ e $r_t < \beta^t \leq n$, temos $d_t > 0$.

Em seguida dividimos $r_t$ por $\beta^{t-1}$ obtendo um quociente $d_{t-1}$ e um resto $r_{t-1}$ tais que

$$r_t = d_{t-1}\beta^{t-1} + r_{t-1} \quad \text{e} \quad r_{t-1} < \beta^{t-1}.$$

Eventualmente pode ocorrer que $d_{t-1}$ seja zero.

Executando esse procedimento num total de $t$ vezes, encontramos quocientes $d_i$ e restos $r_i$ tais que

$$n = d_t\beta^t + r_t \quad \text{e} \quad r_t < \beta^t$$

e

$$r_i = d_{i-1}\beta^{i-1} + r_{i-1} \quad \text{e} \quad r_{i-1} < \beta^{i-1}$$

para todo $i$ tal que $1 \leq i < t$.

Para $i = 2$ temos $r_2 = d_1\beta^1 + r_1$ com $r_1 < \beta$. Para $i = 1$ temos $r_1 = d_0\beta^0 + r_0 = d_0$, sendo exata a divisão por $\beta^0 = 1$. Coletando as identidades acima obtemos

$$\begin{aligned} n &= d_t\beta^t + r_t \\ &= d_t\beta^t + d_{t-1}\beta^{t-1} + r_{t-1} \\ &\vdots \\ &= d_t\beta^t + d_{t-1}\beta^{t-1} + \cdots + d_1\beta + r_1 \\ &= d_t\beta^t + d_{t-1}\beta^{t-1} + \cdots + d_1\beta + d_0. \end{aligned}$$

Notemos que $d_i < \beta$ para todo $0 \leq i \leq t$. De fato, isso é verdade para $i = t$, pois $n < \beta^{t+1} \Rightarrow d_t\beta^t + r_t < \beta^{t+1} \Rightarrow d_t\beta^t < \beta^{t+1} \Rightarrow d_t < \beta$. Seja $i$ tal que $0 \leq i < t$. Temos $r_{i+1} = d_i\beta^i + r_i$ e $r_{i+1} < \beta^{i+1}$. Portanto $d_i\beta^i + r_i < \beta^{i+1} \Rightarrow d_i\beta^i < \beta^{i+1} \Rightarrow d_i < \beta$.

Fica demonstrada a existência da representanção de $n$ na base $\beta$. Passamos agora a demonstrar a unicidade da representação.

Resguardando a representação 6.1, seja $n = f_s\beta^s + f_{s-1}\beta^{s-1} + \cdots + f_1\beta + f_0$ uma representação qualquer, nas condições do enunciado do Teorema.

Como $f_s \neq 0$ segue que $\beta^s \leq n$. Como $f_i \leq \beta - 1$ para todo $i$ segue que $n \leq (\beta-1)\beta^s + (\beta-1)\beta^{s-1} + \cdots + (\beta-1) = (\beta-1)[\beta^s + \beta^{s-1} + \cdots + 1] = (\beta-1)(\beta^{s+1}-1)/(\beta-1) = \beta^{s+1} - 1 < \beta^{s+1}$. Portanto $\beta^s \leq n < \beta^{s+1}$. Como é único o número $t$ tal que $\beta^t \leq n < \beta^{t+1}$ segue que $t = s$.

Observamos de $n = (d_t\beta^{t-1} + d_{t-1}\beta^{t-2} + \cdots + d_1)\beta + d_0$ que $d_t\beta^{t-1} + d_{t-1}\beta^{t-2} + \cdots + d_1$ e $d_0 < \beta$ são respectivamente o quociente e o resto da divisão euclidiana de $n$ por $\beta$.

Observamos ainda de $n = (f_t\beta^{t-1} + f_{t-1}\beta^{t-2} + \cdots + f_1)\beta + f_0$ que $f_t\beta^{t-1} + f_{t-1}\beta^{t-2} + \cdots + f_1$ e $f_0 < \beta$ são também respectivamente o quociente e o resto da divisão euclidiana de $n$ por $\beta$.

Em virtude da unicidade do quociente e do resto da divisão euclidiana temos

$$d_t\beta^{t-1} + d_{t-1}\beta^{t-2} + \cdots + d_1 = f_t\beta^{t-1} + f_{t-1}\beta^{t-2} + \cdots + f_1 \quad \text{e} \quad d_0 = f_0.$$

Aplicando o mesmo argumento a $d_t\beta^{t-1} + d_{t-1}\beta^{t-2} + \cdots + d_1 = f_t\beta^{t-1} + f_{t-1}\beta^{t-2} + \cdots + f_1$ vemos que $d_t\beta^{t-2} + d_{t-1}\beta^{t-3} + \cdots + d_2 = f_t\beta^{t-2} + f_{t-1}\beta^{t-3} + \cdots + f_2$ e $d_1 = f_1$.

Repetindo o argumento até esgotar concluímos que $d_i = f_i$ para todo $i$, terminando a demonstração da unicidade. □

Se o estudante estudar acuradamente a demonstração do Teorema 6.7 deverá perceber que qualquer sequência crescente de números naturais determina um sistema de numeração posicional. Confira o Problema 6.6.14.

## 6.5 Problemas

**Problema 6.5.1.** Construa um argumento, diferente daquele do texto, para verificar que, dados números naturais quaisquer $n \geq 1$ e $\beta \geq 2$, existe um único número natural $t$ tal que $\beta^t \leq n < \beta^{t+1}$.

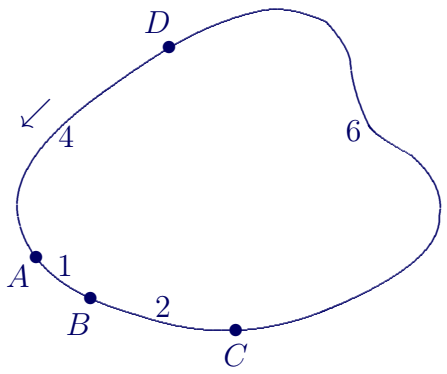
**Problema 6.5.2.** Demonstre que todo sistema de numeração aditivo de base $\beta$ satisfaz às propriedades fundamentais de existência e unicidade.

**Problema 6.5.3.** Demonstre que todo número natural $n > 0$ se escreve como uma soma de diferentes potências de 2. Prove que essa representação é única.

## 6.6 Problemas adicionais

**Problema 6.6.1.** Os campeonatos mundiais de futebol são realizados de quatro em quatro anos a partir de 1930 (não houve certames em 1942 e em 1946). Supondo que essa prática continue regularmente, pergunta-se se haverá campeonato mundial de futebol no ano de 4472. Justifique.

**Problema 6.6.2.** A figura representa o traçado de uma pista de corrida. Os postos $A$, $B$, $C$ e $D$ são usados para partidas e chegadas de todas as corridas. As distâncias entre postos vizinhos, em quilômetros, estão indicadas na figura, e as corridas são realizadas no sentido indicado pela seta. Por exemplo, uma corrida de 17 quilômetros pode ser realizada com partida em $D$ e chegada em $A$. Mostre que é possível realizar corridas com extensão em quilômetros igual a qualquer número natural.



**Problema 6.6.3.** Os números naturais de 1 a 1000 são escritos em ordem em volta de uma circunferência. Começando com 1 e dando voltas na circunferência, marque os números 1, 15, 29, 43, ..., contando de quatorze em quatorze, só parando no momento em que for atingido um número já marcado. Determine quais foram os números não marcados.

**Problema 6.6.4.** Verifique que se 3 divide $a^2 + b^2$ então 3 divide $a$ e $b$, quaisquer que sejam os números naturais $a$ e $b$.

**Problema 6.6.5.** Observe que se $n$ e $a$ são números naturais positivos com $a$ ímpar, então $(a^n - 1)/2$ é um número natural. Investigue a paridade desse número. Isto é, determine em que condições sobre $a$ e $n$ o número $(a^n - 1)/2$ é par (e, complementarmente, é ímpar).

**Problema 6.6.6.** Determine todos os números naturais $a$ para os quais 10 divide $a^{10} + 1$.

**Problema 6.6.7.** Aproveitando que definimos no texto a notação $\lfloor x \rfloor$, verifique as duas propriedades seguintes. **a)** Quaisquer que sejam os números reais $x \geq 0$ e $y \geq 0$, temos $\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x + y \rfloor$. **b)** Para todo número real $x \geq 0$ e para todo número natural $n \geq 1$ vale que

$$\left\lfloor \frac{\lfloor x \rfloor}{n} \right\rfloor = \left\lfloor \frac{x}{n} \right\rfloor$$

**Problema 6.6.8.** Vamos dar continuidade ao Problema 5.5.7. Como antes, dado um algoritmo de primaridade $\mathcal{A}$ e dado um número natural $n$, indicamos por $\mathcal{A}(n)$ a quantidade máxima de divisões necessárias para, usando o algoritmo $\mathcal{A}$, determinar se $n$ é primo ou não.
**d)** Dado um número natural $n \geq 2$, sabe-se que ele não é múltiplo de 2, 3 ou 5. Calcule $\mathcal{A}(n)$ para o seguinte algoritmo de primaridade $\mathcal{A}$: dividir $n$ pelos números 2, ..., $n - 2$ que não são múltiplos de 2, nem de 3 e nem de 5; se nenhuma das divisões for exata, então $n$ é primo. Sugestão: use a notação e a ideia do Problema Resolvido 6.6.
**e)** Dado um número natural $n \geq 2$, sabe-se que ele não é múltiplo de 2, 3 ou 5. Calcule $\mathcal{A}(n)$ para o seguinte algoritmo de primaridade $\mathcal{A}$: dividir $n$ pelos números 2, ..., $[\sqrt{n}\,]$ que não são múltiplos de 2, nem de 3 e nem de 5; se nenhuma das divisões for exata, então $n$ é primo.
**f)** Usando o algoritmo anterior, quantas divisões você precisaria fazer, no máximo, para verificar se $n = 1\,000\,003$ é primo ou não?

**Problema 6.6.9.** Para todo número natural $a \geq 10$, indicamos por $s(a)$ a soma dos dígitos decimais de $a$. Se $a = 9$ poremos $s(9) = 0$. Por exemplo, $s(173) = 1 + 7 + 3 = 11$. **a)** Prove que para todo $a \geq 9$ o número $s(a)$ é um resto da divisão de $a$ por 9, mas não necessariamente é o resto da divisão euclidiana de $a$ por 9. **b)** Ponhamos $s^1(a) = s(a)$ e $s^m(a) = s(s^{m-1}(a))$ para todo número natural $m \geq 2$. Demonstre que para todo $a$ existe $m$ tal que $s^m(a) = 9$ ou $s^m(a)$ é o resto da divisão euclidiana de $a$ por 9.

**Problema 6.6.10.** Para todo número natural $a$, indicamos por $r(a)$ o resto da divisão euclidiana de $a$ por 9. **a)** (*prova do nove para a adição*) Demonstre que $r(r(a) + r(b)) = r(a + b)$, quaisquer que sejam os números naturais $a$ e $b$. **b)** (*prova do nove para a multiplicação*) Demonstre que $r(r(a)r(b)) = r(ab)$, quaisquer que sejam os números naturais $a$ e $b$.

**Problema 6.6.11.** A numeração das horas, minutos e segundos do dia pode ser definida por um sistema posicional da forma $(h; m; s)_{horas}$, em que $0 \leq h < 24$, $0 \leq m < 60$ e $0 \leq s < 60$ são números naturais representados no sistema decimal, e $(h; m; s)_{horas} = h$ horas $m$ minutos e $s$ segundos. Portanto 1 minuto equivale a 60 segundos, uma hora a 60 minutos e 1 dia a 24 horas. **a)** Um dia tem 86400 segundos. Demonstre que todo número natural $0 \leq n < 86400$ tem uma única representação no sistema acima. **b)** Usando a aritmética desse sistema faça os cálculos: 17h32m12s+2h47m51s; 23h19m8s−5h38m42s; 3×7h17m37s; 6h37m40s÷4.

**Problema 6.6.12.** Em Geometria e em Astronomia se mede o ângulo central de uma circunferência em graus, minutos de arco e segundos de arco. Um grau vale 60 minutos de arco, e este vale 60 segundos de arco. Uma volta inteira na circunferência vale 360 graus. Anotamos, como é costume, $x$ graus por $x^\circ$, $y$ minutos de arco por $y'$ e $z$ segundos de arco por $z''$. Se um ponto deu $u$ voltas inteiras em uma circunferência, indicamos por $u^v$. **a)** Escreva a forma expandida do sistema $u^v x^\circ y' z''$. Ele é posicional? **b)** Efetue nesse sistema $3^v 150^\circ 38' 52'' + 2^v 217^\circ 47' 29''$.

**Problema 6.6.13.** **a)** Demonstre que todo número natural $a \geq 2$ pode ser escrito na forma

$$a = 3^n + a_{n-1}3^{n-1} + \ldots + a_2 3^2 + a_1 3 + a_0$$

em que $n \geq 1$ e $a_i = -1$, 0 ou 1 para todo $i = 0, 1, 2, ..., n-1$, denominada *expansão ternária balanceada*. **b)** Demonstre que a expansão ternária balanceada de qualquer número natural $a \geq 2$ é única. **c)** Seja $n \geq 1$ um número natural. Prove que a expansão ternária balanceada de todo número natural $a$ tal que $2 \leq a \leq (3^{n+1} - 1)/2$ é da forma $a = 3^m + a_{m-1}3^{m-1} + \ldots + a_2 3^2 + a_1 3 + a_0$, com $a_i = -1$, 0 ou 1 para todo $i = 0, 1, 2, ..., m-1$ e com $m \leq n$.

**Problema 6.6.14.** Seja $\beta_0 = 1 < \beta_1 < \beta_2 < \beta_3 < \ldots < \beta_m < \ldots$ uma sequência infinita de números naturais. Qualquer número natural $n \geq 1$ se escreve na forma

$$n = d_t\beta_t + d_{t-1}\beta_{t-1} + \cdots + d_1\beta_1 + d_0 \tag{6.3}$$

para algum $t$ e com dígitos $d_i$ tais que $0 < d_t$ e $0 \leq d_i < \beta_{i+1}/\beta_i$ para $i = 0, 1, 2, \ldots, t$. Além disso, se $d_i\beta_i + d_{i-1}\beta_{i-1} + \ldots + d_0\beta_0 < \beta_{i+1}$ para todo $i \geq 0$, então a representação é única. Com pequenas adaptações, a sequência $(\beta_m)$ pode ser finita.

## 6.7 Temas para investigação

**Tema 6.7.1.** Dado um número natural $a \geq 1$, investigue como é a unidade da representação decimal de $a^n$ para todo número natural $n \geq 1$. Faça conjecturas. Alguma demonstração?

**Tema 6.7.2.** Um estudante, examinando alguns primos $p > 5$, fez a seguinte conjectura: "$p > 5$ é primo se e somente se é de uma das formas $p = 6k + 1$ ou $p = 6k + 5$, sendo $k$ qualquer número natural." Demonstre a conjectura ou, se estiver errada, faça um ajuste para torná-la verdadeira.

**Tema 6.7.3.** Considere os seguintes eventos:

$$\begin{array}{ll}
2^1 + 1 = 3 & 2^{10} + 1 = 5^2 \cdot 41 \\
2^2 + 1 = 5 & 2^{11} + 1 = 3 \cdot 683 \\
2^3 + 1 = 3^2 & 2^{12} + 1 = 17 \cdot 241 \\
2^4 + 1 = 17 & 2^{13} + 1 = 3 \cdot 2731 \\
2^5 + 1 = 3 \cdot 11 & 2^{14} + 1 = 5 \cdot 29 \cdot 113 \\
2^6 + 1 = 5 \cdot 13 & 2^{15} + 1 = 3^2 \cdot 11 \cdot 331 \\
2^7 + 1 = 3 \cdot 43 & 2^{16} + 1 = 65537 \\
2^8 + 1 = 257 & 2^{17} + 1 = 3 \cdot 43691 \\
2^9 + 1 = 3^3 \cdot 19 & 2^{18} + 1 = 5 \cdot 13 \cdot 37 \cdot 109
\end{array}$$

**a)** Observe as regularidades. Alguma conjectura? Alguma demonstração?

**b)** Generalize. Calcule os divisores de $n^j + 1$ para outros valores de $n$, como $n = 3$, $n = 4$, etc. Quais das regularidades observadas em a) permanecem? Outras conjecturas? Demonstrações?

# Capítulo 7

# O Teorema Fundamental da Aritmética

## 7.1 Introdução

O Teorema Fundamental da Aritmética estabelece a existência e unicidade da decomposição de todo número natural $n \geq 2$ como produto de primos. Esse é um resultado importante da Teoria dos Números. Neste capítulo demonstramos esse teorema e apresentamos algumas aplicações.

## 7.2 Propriedades adicionais do máximo divisor comum

Uma das formas de demonstrar o Teorema Fundamental da Aritmética consiste em utilizar certas propriedades do mdc. Vimos na Seção 5.10 a definição do mdc de dois ou mais números naturais e estudamos várias propriedades. Vamos ampliar esse estudo com alguns resultados adicionais. A apresentação que segue nesta seção é um detalhamento de [119], páginas 2 a 8.

Vimos no Escólio 5.16 que "se $a$, $b$, $q$ e $r$ são números naturais tais que $a = bq + r$, então os divisores comuns de $a$ e $b$ são também os divisores comuns de $b$ e $r$". Aplicamos esse resultado para construir o algoritmo euclidiano para o cálculo do mdc de números naturais. Mas essa construção nos fornece outras propriedades.

Sejam $a$ e $b \neq 0$ números naturais. Dividindo $a$ por $b$ encontramos números naturais $q_1$ e $r_1$ tais que $a = bq_1 + r_1$ e $0 \leq r_1 < b$. Se $0 < r_1$, dividimos $b$ por $r_1$ e encontramos números naturais $q_2$ e $r_2$ tais que $b = r_1q_2 + r_2$ e $0 \leq r_2 < r_1$. E assim sucessivamente, no $i$-ésimo passo dividimos $r_{i-2}$ por $r_{i-1}$ e encontramos números naturais $q_i$ e $r_i$ tais que $r_{i-2} = r_{i-1}q_i + r_i$ e $0 \leq r_i < r_{i-1}$. Obtemos assim uma sequência de restos $0 < \ldots < r_i < \ldots < r_3 < r_2$ enquanto $r_i$ não for nulo. Mas entre $b$ e 0 existe uma quantidade finita de números naturais. Assim esse procedimento necessariamente nos fornece um resto $r_{n+1} = 0$, de modo que $r_n$ é divisor de $r_{n-1}$. Em resumo temos as relações:

$$\begin{array}{rcll} a & = & bq_1 + r_1 & 0 \leq r_1 < b \\ b & = & r_1q_2 + r_2 & 0 \leq r_2 < r_1 \\ r_1 & = & r_2q_3 + r_3 & 0 \leq r_3 < r_2 \\ \vdots & & & \\ r_{n-2} & = & r_{n-1}q_n + r_n & 0 \leq r_n < r_{n-1} \\ r_{n-1} & = & r_nq_{n+1} + r_{n+1} & 0 = r_{n+1} \end{array} \tag{7.1}$$

Conforme já sabemos, uma consequência dessas identidades e do Teorema 5.15 é que $\text{mdc}(a,b) = r_n$. Agora, como resultado do Escólio 5.16, temos o

**Teorema 7.1.** *Se $a$ e $b$ são números naturais, então o conjunto dos divisores comuns de $a$ e $b$ é também o conjunto dos divisores de* $\text{mdc}(a,b)$. *Ou seja, $\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(\text{mdc}(a,b))$.*

*Demonstração.* Se $b = 0$ o conjunto dos divisores comuns de $a$ e $b$ é $\mathcal{D}(a)$. Como $\text{mdc}(a,0) = a$, vale a afirmação do Teorema. Suponhamos $b \neq 0$. As identidades 7.1 e o Escólio 5.16 nos dizem que $\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(b) \cap \mathcal{D}(r_1) = \mathcal{D}(r_1) \cap \mathcal{D}(r_2) = \ldots = \mathcal{D}(r_{n-1}) \cap \mathcal{D}(r_n)$. Como $r_n$ é divisor de $r_{n-1}$ temos $\mathcal{D}(r_{n-1}) \cap \mathcal{D}(r_n) = \mathcal{D}(r_n)$. Portanto $\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(r_n)$. Lembrando que $\text{mdc}(a,b) = r_n$, terminamos a demonstração. □

A esse respeito confira os Problemas 5.11.16 e 5.11.17. Vejamos agora o

**Teorema 7.2.** *Para todo número natural $t$ vale*

$$\text{mdc}(ta, tb) = t\,\text{mdc}(a,b) \tag{7.2}$$

*quaisquer que sejam os números naturais $a$ e $b$.*

*Demonstração.* Se $t = 0$ temos $\text{mdc}(ta,tb) = \text{mdc}(0,0) = 0$ e $t\,\text{mdc}(a,b) = 0\,\text{mdc}(a,b) = 0$, e vale a afirmação. Suponhamos $t > 0$. Se $b = 0$, temos $\text{mdc}(ta,0) = ta$ e $t\,\text{mdc}(a,0) = ta$, e vale a afirmação. Suponhamos que $b \neq 0$. Consideremos as identidades 7.1. Elas nos dizem que $\text{mdc}(a,b) = r_n$. Ainda, multiplicando as identidades e desigualdades 7.1 por $t$ vem

$$\begin{array}{rcll} ta & = & tbq_1 + tr_1 & 0 \leq tr_1 < tb \\ tb & = & tr_1q_2 + tr_2 & 0 \leq tr_2 < tr_1 \\ tr_1 & = & tr_2q_3 + tr_3 & 0 \leq tr_3 < tr_2 \\ \vdots & & & \\ tr_{n-2} & = & tr_{n-1}q_n + tr_n & 0 \leq tr_n < tr_{n-1} \\ tr_{n-1} & = & tr_nq_{n+1} + tr_{n+1} & 0 = tr_{n+1} \end{array} \tag{7.3}$$

o que nos diz que $\text{mdc}(ta,tb) = tr_n$. Portanto $\text{mdc}(ta,tb) = t\,\text{mdc}(a,b)$. Isso termina a demonstração do Teorema. □

Segue um resultado importante, um dos principais objetivos desta seção:

**Teorema 7.3.** *Se* $\text{mdc}(a,b) = 1$ *e se $b$ é divisor de $ac$ então $b$ é divisor de $c$, quaisquer que sejam os números naturais $a$, $b > 0$ e $c$.*

*Demonstração.* Aplicando o Teorema 7.2 temos $\text{mdc}(ac,bc) = c\,\text{mdc}(a,b) = c$. Por outro lado, como $b$ é divisor de $ac$ e de $bc$, em virtude do Teorema 7.1 $b$ é divisor de $\text{mdc}(ac,bc)$. Segue que $b$ é divisor de $c$. □

**Corolário 7.4.** *Se $p$ é primo e se $p$ é divisor de $ab$ então $p$ é divisor de $a$ ou de $b$, quaisquer que sejam os números naturais $a$ e $b$.*

*Demonstração.* Se $p$ é divisor de $a$ nada há a demonstrar. Suponhamos que $p$ não é divisor de $a$. Então $\text{mdc}(p,a) = 1$, e o Teorema acima garante que $p$ é divisor de $b$. □

Esse importante Corolário tem diversas demonstrações, por exemplo confira o Problema 7.10.12. Confira também [49], páginas 58 a 62.

**Corolário 7.5.** *Se $p$, $q$ e $t$ são primos e se $p$ é divisor de $qt$ então $p = q$ ou $p = t$.*

*Demonstração.* Devido ao Corolário anterior, $p$ é divisor de $q$ ou de $t$. Então $p = q$ ou $p = t$. □

O resultado abaixo é uma generalização do Corolário 7.4.

**Corolário 7.6.** *Se $p$, $a_1$, $a_2$, ..., $a_s$ são números naturais com $p$ primo e se $p$ é divisor do produto $a_1a_2 \cdots a_s$ então existe $i$, com $1 \leq i \leq s$, tal que $p$ é divisor de $a_i$.*

*Demonstração.* Se $s = 1$ a afirmação é trivial. Se $s = 2$, segue do Corolário 7.4. Seja $s \geq 3$. Como $p$ é divisor de $a_1a_2 \cdots a_s = (a_1a_2 \cdots a_{s-1})a_s$, então, pelo mesmo Corolário, $p$ é divisor de $a_1a_2 \cdots a_{s-1}$ ou de $a_s$. Se ocorrer esse último caso, terminamos. Caso contrário, $p$ é divisor de $a_1a_2 \cdots a_{s-1}$. Reaplicando o procedimento um número finito de vezes, obtemos que $p$ é divisor de $a_1a_2$. Pelo mesmo Corolário já citado, $p$ divide $a_1$ ou $a_2$, e terminamos. □

O seguinte resultado é bastante útil.

**Teorema 7.7.** *Sejam $a \neq 0$ e $b \neq 0$ números naturais relativamente primos. Se $a$ e $b$ são divisores do número natural $c$ então $ab$ também o é.*

*Demonstração.* Temos $\text{mdc}(ac, bc) = c\,\text{mdc}(a, b) = c$. Como $ab$ é divisor de $ac$ e de $bc$ vem que $ab$ é divisor de $\text{mdc}(ac, bc)$, e portanto de $c$. □

**Problema resolvido 7.8.** Se $\text{mdc}(a, b) = 1$ então $\text{mdc}(ac, b) = \text{mdc}(c, b)$ quaisquer que sejam os números naturais $a$, $b$ e $c$.

*Solução.* Se $c = 0$ temos $\text{mdc}(ac, b) = b$ e $\text{mdc}(c, b) = b$, e vale a afirmação. Suponhamos $c > 0$. Se $a = 0$ temos $b = 1$ em virtude da condição $\text{mdc}(a, b) = 1$. Então $\text{mdc}(ac, b) = b = 1$ e $\text{mdc}(c, b) = \text{mdc}(c, 1) = 1$, e vale a afirmação. Se $b = 0$ temos $a = 1$ em virtude da condição $\text{mdc}(a, b) = 1$. Então $\text{mdc}(ac, b) = \text{mdc}(c, b)$, e novamente vale a afirmação. Suponhamos $a > 0$ e $b > 0$. Seja $d = \text{mdc}(ac, b)$. Temos $d \geq 1$ e $d$ é divisor comum de $ac$ e de $b$, o que implica ser $d$ divisor comum de $ac$ e de $bc$. Então $d$ é divisor de $\text{mdc}(ac, bc)$, em virtude do Teorema 7.1. Mas $\text{mdc}(ac, bc) = c\,\text{mdc}(a, b)$, conforme vimos no Teorema 7.2. Usando a hipótese $\text{mdc}(a, b) = 1$ segue que $d$ é divisor de $c$. Portanto $d$ é divisor comum de $c$ e $b$, e assim $d$ é divisor de $\text{mdc}(c, b)$.

Por outro lado, seja $f = \text{mdc}(c, b)$. Então $f \geq 1$ e $f$ é divisor de $c$ e de $b \Rightarrow f$ é divisor de $ac$ e de $b \Rightarrow f$ é divisor de $\text{mdc}(ac, b)$.

Provamos que $d$ é divisor de $f$ e vice-versa. Como $d \geq 1$ e$f \geq 1$ obtemos $d \leq f$ e $f \leq d$, portanto $d = f$. Isso termina a demonstração. □

## 7.3 Problemas

**Problema 7.3.1.** Demonstre a afirmação recíproca do Corolário 7.4. Suponha que o número natural $p > 1$ satisfaça à seguinte condição: quaisquer que sejam os números naturais $a$ e $b$, se $p$ divide $ab$ então $p$ divide $a$ ou $p$ divide $b$. Prove que com essa condição $p$ é primo.

**Problema 7.3.2.** Demonstre novamente o critério de divisibilidade por 6 dado no Problema 4.10.25, mas agora utilizando os resultados desta seção.

**Problema 7.3.3.** Demonstre uma versão mais geral do Teorema 7.2: para todo número natural $t$ e quaisquer que sejam os números naturais $a_1$, $a_2$, ..., $a_n$, tem-se $\text{mdc}(ta_1, \ldots, ta_n) = t\,\text{mdc}(a_1, \ldots, a_n)$.

**Problema 7.3.4.** Se $p$, $p_1$, $p_2$, ..., $p_s$ são primos e se $p$ é divisor do produto $p_1p_2\dots p_s$ então $p = p_i$ para algum $i$.

**Problema 7.3.5.** Se $p$ é primo e se $p$ é divisor de $a^n$, então $p$ é divisor de $a$, quaisquer que sejam os números naturais $a$ e $n \geq 1$.

**Problema 7.3.6.** Se $p$ é primo e se $p$ é divisor de $a^n$, então $p^n$ é divisor de $a^n$, quaisquer que sejam os números naturais $a$ e $n \geq 1$.

**Problema 7.3.7.** **a)** Exiba divisores de 91! que são $> 91$. Qual é o menor? **b)** Exiba o maior divisor de 91! que não seja ele mesmo. **c)** Encontre todos os números primos divisores de 91! Justifique.

**Problema 7.3.8.** Se $p$ e $q$ são primos e se $p$ é divisor de $q^n$ então $p = q$.

**Problema 7.3.9.** Prove que se $n = p^2$ com $p$ primo, então $\mathcal{D}(n) = \{1, p, n\}$.

**Problema 7.3.10.** Demonstre que se $n = pq$ com $p$ e $q$ primos, então $\mathcal{D}(n) = \{1, p, q, n\}$.

**Problema 7.3.11.** Se $a$, $b$, $c$ e $n$ são números naturais tais que $a$ e $c$ são relativamente primos e $a$ é divisor de $bc^n$, então $a$ é divisor de $b$.

**Problema 7.3.12.** Sejam $a$ e $b$ números naturais não simultaneamente nulos. Seja $\text{mdc}(a, b) = d$ e sejam $a_1$ e $b_1$ tais que $a = da_1$ e $b = db_1$. Mostre que $\text{mdc}(a_1, b_1) = 1$.

**Problema 7.3.13.** Prove que se $a \neq 0$ e $b \neq 0$ são números naturais relativamente primos e se $c$ é um divisor de $ab$, então existem números naturais relativamente primos $c_1$ e $c_2$ tais que $c = c_1c_2$, $c_1$ é divisor de $a$ e $c_2$ é divisor de $b$.

**Problema 7.3.14.** Demonstre que se $p$ é primo então $p$ não divide $n!$ para todo número natural $n$ tal que $n < p$.

**Problema 7.3.15.** Investigue para quais números naturais $n \geq 1$ é verdade que $n$ é divisor de $(n-1)!$ Alguma justificativa?

**Problema 7.3.16.** Se $p$ é primo então $p$ divide $\binom{p}{i}$ para todo número natural $i$ tal que $0 < i < p$.

## 7.4 O Teorema Fundamental da Aritmética

Para alguns autores o Teorema Fundamental da Aritmética (TFA) é o resultado do Corolário 7.4: Se $p$ é primo e se $p$ é divisor de $ab$ então $p$ é divisor de $a$ ou de $b$, quaisquer que sejam os números naturais $a$ e $b$. Para outros autores é o seguinte

**Teorema 7.9.** *Todo número natural $\geq 2$ é primo ou pode ser decomposto como um produto de números primos, e essa decomposição é única a menos da ordem dos fatores.*

*Demonstração.* Vimos no Teorema 4.22 que todo número natural $\geq 2$ é primo ou se escreve como produto de primos. Vejamos agora a unicidade. Seja $n \geq 2$ um número natural, e sejam

$$n = p_1p_2p_3\dots p_s = q_1q_2q_3\dots q_t$$

decomposições de $n$ como produto de primos. Queremos provar que $s = t$ e que, rearranjando os índices se necessário, $p_i = q_i$ para todo $i$ tal que $1 \leq i \leq s$.

Sem perda de generalidade suponhamos que $s \leq t$. Como $p_1$ é divisor de $q_1 q_2 q_3 \dots q_t$, pelo Corolário 7.6 existe $j$ tal que $p_1 \mid q_j$, logo $p_1 = q_j$. Rearranjando os índices de $q_1 q_2 q_3 \dots q_t$, podemos supor que $p_1 = q_1$. Temos agora $p_2 p_3 \dots p_s = q_2 q_3 \dots q_t$. Reaplicando o procedimento um número finito de vezes, chegamos a $p_i = q_i$ para $1 \leq i \leq s$ e $1 = q_{s+1} \cdots q_t$. Mas então $s = t$, e terminamos. □

Conforme já observamos na Definição 4.25, na decomposição de um número natural qualquer $n \geq 2$ como produto de primos podemos reunir em potências os primos iguais e escrever

$$n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \dots p_s^{e_s} \tag{7.4}$$

em que cada $p_i$ é um primo diferente dos outros e cada $e_i$ é um número natural positivo.

Lembramos que a forma 7.4 se denomina *decomposição canônica* de $n$. Nesse contexto a unicidade da decomposição significa que se

$$n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \dots p_s^{e_s} = q_1^{f_1} q_2^{f_2} q_3^{f_3} \dots q_t^{f_t}$$

são decomposições canônicas de $n$, então $s = t$, $p_i = q_i$ e $e_i = f_i$ para todo $i$ tal que $1 \leq i \leq s$ (com rearranjo dos índices, se necessário).

**Problema resolvido 7.10.** Sejam $a$ e $b$ números naturais. Demonstre que se $2^a + 1 = b^2$ então $a = b = 3$.

*Solução.* Notemos que $b > 1$ e que $2^a = b^2 - 1 = (b+1)(b-1)$. Como $2^a$ é par então necessariamente $b$ é ímpar. Existe um número natural $k \geq 1$ tal que $b = 2k + 1$. Temos $2^a = (b+1)(b-1) = 4k(k+1)$. Em virtude do Teorema Fundamental da Aritmética, 2 é o único primo da decomposição de $4k(k+1)$ em primos.

Afirmamos que $k = 1$. Suponhamos $k > 1$. Sendo $k$ e $k+1$ números consecutivos, um deles é ímpar e $> 1$, e portanto tem um divisor primo ímpar. Mas isso é uma contradição. Segue que $k = 1$ e $b = 3$. De $2^a + 1 = 3^2$ vem $a = 3$. □

## 7.5 Problemas

**Problema 7.5.1.** Determine as decomposições canônicas de 585 e 23100.

**Problema 7.5.2.** Usando o Teorema Fundamental da Aritmética, determine o menor número natural positivo $m$ tal que $315 \cdot m$ é um quadrado perfeito.

**Problema 7.5.3.** Demonstre que todo número natural $n \geq 1$ se escreve de maneira única na forma $n = 2^a b$, em que $a \geq 0$ é um número natural e $b \geq 1$ é ímpar.

**Problema 7.5.4. a)** Prove que se $n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \dots p_s^{e_s}$ é a decomposição canônica de $n$ como produto de primos, então $n$ é um quadrado perfeito se e somente se $e_i$ é par para todo $1 \leq i \leq s$. **b)** Prove que se $n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \dots p_s^{e_s}$ é a decomposição canônica de $n$ como produto de primos, então $n$ é a $k$-ésima potência de um número natural se e somente se $e_i$ é múltiplo de $k$ para todo $1 \leq i \leq s$.

**Problema 7.5.5.** Demonstre que, para todo número natural $n$, $n^3$ é um quadrado perfeito se e somente se $n$ é um quadrado. Além disso, se $n^3 = m^2$ então $m$ é um número cúbico e $\sqrt[3]{m} = \sqrt[2]{n}$.

**Problema 7.5.6.** Uando o Teorema Fundamental da Aritmética demonstre que se $p$ é primo então não existem números naturais positivos $a$ e $b$ tais que $a^2 = pb^2$.

**Problema 7.5.7.** Sejam $a$, $b$ e $n \geq 1$ números naturais. Prove que se $a^n$ divide $b^n$ então $a$ divide $b$.

**Problema 7.5.8.** Consideremos o conjunto $S = \{1, 4, 7, 10, \ldots\}$ formado pelos números da forma $1+3k$, $k \geq 0$. $S$ é fechado em relação à multiplicação. Dizemos que um número $a > 1$ de $S$ é *primo em* $S$ quando não pode ser decomposto na forma $a = bc$ com $b > 1$ e $c > 1$ elementos de $S$. **a)** Prove que todo elemento $a > 1$ de $S$ é primo em $S$ ou é produto de primos em $S$. **b)** Verifique que em $S$ não vale a unicidade da decomposição em produto de primos.

## 7.6 Aplicações

Uma importante aplicação é:

**Teorema 7.11.** *Se $a$ e $b$ são números naturais relativamente primos e se $ab = m^2$ para algum número natural $m$, então $a$ e $b$ são quadrados perfeitos.*

*Demonstração.* Se $a = 1$ ou $b = 1$ o resultado é claro. Suponhamos $a > 1$ e $b > 1$. Seja $p$ um primo que divide $a$, e seja $e$ o expoente de $p$ na decomposição canônica de $a$. Naturalmente $p$ é um divisor de $m$, e $p$ comparece na decomposição canônica de $m^2$ com expoente par, digamos $2f$. Como $p$ não é divisor de $b$ e $ab = m^2$, temos $p^e = p^{2f}$, em virtude da unicidade da decomposição garantida pelo TFA. Isso implica $e = 2f$. Fica provado que na decomposição canônica de $a$ os expoentes são todos pares, e assim $a$ é um quadrado perfeito. O mesmo resultado se aplica a $b$. □

O Teorema Fundamental da Aritmética nos fornece um método para contar e listar os divisores de um número natural. Vejamos primeiro uma caracterização desses divisores.

**Teorema 7.12.** *Se $n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \ldots p_s^{e_s}$ é a decomposição canônica do número natural $n > 1$ então $m$ é divisor de $n$ se e somente se é da forma $m = p_1^{f_1} p_2^{f_2} p_3^{f_3} \ldots p_s^{f_s}$ com $0 \leq f_i \leq e_i$ para todo $i$.*

*Demonstração.* Se $m = p_1^{f_1} p_2^{f_2} p_3^{f_3} \ldots p_s^{f_s}$ com $0 \leq f_i \leq e_i$ para todo $i$ então

$$n = m \left( p_1^{e_1 - f_1} p_2^{e_2 - f_2} p_3^{e_3 - f_3} \ldots p_s^{e_s - f_s} \right)$$

e portanto $m$ é divisor de $n$.

Reciprocamente seja $m$ um divisor de $n$. Os únicos primos que podem comparecer na decomposição canônica de $m$ são os primos $p_i$. Portanto podemos escrever $m = p_1^{f_1} p_2^{f_2} p_3^{f_3} \ldots p_s^{f_s}$ com $0 \leq f_i$ (se algum $p_i$ não comparece isso significa que $f_i = 0$). Como $p_i^{f_i}$ divide $n$ então $f_i \leq e_i$. Isso termina a demonstração. □

Notemos que 1 é um divisor de $n$ e 1 é da forma requerida pelo Teorema 7.12, pois se escreve como $1 = p_1^0 p_2^0 p_3^0 \ldots p_s^0$, com $f_i = 0$ para todo $i$. Se $f_i = e_i$ para todo $i$ temos o caso em que o divisor é o próprio $n$.

O Teorema 7.12 nos dá um método para contar a quantidade de divisores de $n$. Observando a forma dos divisores de $n$, vemos que cada primo $p_i$ comparece com expoentes que vão de 0 a $e_i$, portanto, com $e_i + 1$ expoentes diferentes. Assim para cada uma das $e_1 + 1$ escolhas

de $p_1^{f_1}$, com $0 \leq f_1 \leq e_1$, podemos escolher $e_2 + 1$ potências de $p_2$, e para cada uma dessas escolhas podemos escolher $e_3 + 1$ potências de $p_3$, e assim sucessivamente. Isso nos dá um total de $(e_1 + 1)(e_2 + 1) \ldots (e_s + 1)$ divisores de $n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \ldots p_s^{e_s}$.

**Problema resolvido 7.13.** Calcule a quantidade de divisores de 1008.

*Solução.* Como $1008 = 2^4 3^2 7^1$ então a quantidade de divisores é $(4 + 1)(2 + 1)(1 + 1) = 30$. □

Vamos listar organizadamente os divisores de 1008 como uma ilustração da observação acima.

$$\begin{array}{cccccc}
2^0 3^0 7^0 & 2^0 3^1 7^0 & 2^0 3^2 7^0 & 2^0 3^0 7^1 & 2^0 3^1 7^1 & 2^0 3^2 7^1 \\
2^1 3^0 7^0 & 2^1 3^1 7^0 & 2^1 3^2 7^0 & 2^1 3^0 7^1 & 2^1 3^1 7^1 & 2^1 3^2 7^1 \\
2^2 3^0 7^0 & 2^2 3^1 7^0 & 2^2 3^2 7^0 & 2^2 3^0 7^1 & 2^2 3^1 7^1 & 2^2 3^2 7^1 \\
2^3 3^0 7^0 & 2^3 3^1 7^0 & 2^3 3^2 7^0 & 2^3 3^0 7^1 & 2^3 3^1 7^1 & 2^3 3^2 7^1 \\
2^4 3^0 7^0 & 2^4 3^1 7^0 & 2^4 3^2 7^0 & 2^4 3^0 7^1 & 2^4 3^1 7^1 & 2^4 3^2 7^1
\end{array}$$

A quantidade de divisores de um número natural, assim como a soma desses divisores, têm um papel importante na Teoria dos Números, de modo que destacamos essas funções na

**Definição 7.14.** A função $\tau : \mathbb{N}^* \mapsto \mathbb{N}$ definida por $\tau(n) =$ *quantidade de divisores de* $n$ chama-se *função tau*. A função $\sigma : \mathbb{N}^* \mapsto \mathbb{N}$ definida por $\sigma(n) =$ *soma dos divisores de* $n$ chama-se *função sigma*.

**Teorema 7.15.** *Se* $n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \ldots p_s^{e_s}$ *então*

$$\tau(n) = (e_1 + 1)(e_2 + 1) \ldots (e_s + 1) \tag{7.5}$$

*e*

$$\sigma(n) = \frac{p_1^{e_1+1} - 1}{p_1 - 1} \frac{p_2^{e_2+1} - 1}{p_2 - 1} \cdots \frac{p_s^{e_s+1} - 1}{p_s - 1} \tag{7.6}$$

*Demonstração.* A fórmula para $\tau(n)$ já foi comentada. Quanto a $\sigma(n)$ observe que

$$\sigma(n) = (1 + p_1 + p_1^2 + \ldots + p_1^{e_1}) \cdots (1 + p_s + p_s^2 + \ldots + p_s^{e_s})$$

A fórmula 7.6 para $\sigma(n)$ segue da expressão da soma dos termos de uma progressão geométrica. □

Pode ser útil para o estudante decifrar o

**Teorema 7.16.** *Sejam* $n$ *e* $m$ *números naturais quaisquer e escrevamos* $n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \ldots p_s^{e_s}$ *e* $m = p_1^{f_1} p_2^{f_2} p_3^{f_3} \ldots p_s^{f_s}$ *como produto de primos, sendo* $p_1$, $p_2$, ..., $p_s$ *primos diferentes dois a dois e* $e_i \geq 0$ *e* $f_i \geq 0$ *para todo* $i$. *Então*

$$\text{mdc}(n, m) = p_1^{g_1} p_2^{g_2} p_3^{g_3} \ldots p_s^{g_s}$$

*e*

$$\text{mmc}(n, m) = p_1^{h_1} p_2^{h_2} p_3^{h_3} \ldots p_s^{h_s}$$

*com* $g_i = min\{e_i, f_i\}$ *e* $h_i = max\{e_i, f_i\}$ *para todo* $i$.

*Demonstração.* Exercício para o estudante. Observamos que dois números $n$ e $m$ podem ser expressos pelo produto dos mesmos primos, com expoente nulo nos primos que não são comuns. Assim $24 = 2^3 \cdot 3$ e $26 = 2 \cdot 13$ podem ser escritos $24 = 2^3 \cdot 3 \cdot 13^0$ e $26 = 2 \cdot 3^0 \cdot 13$. Esse expediente visa facilitar certos procedimentos, como o enunciado deste Teorema. □

Aproveitamos a oportunidade para apresentar uma propriedade do mmc. Se $b \neq 0$ é um divisor de $a$ uma forma de economizar notação consiste em indicar por $\frac{a}{b}$ o quociente de $a$ por $b$. Isto é, $\frac{a}{b}$ é o número natural $q$ tal que $a = bq$.

**Teorema 7.17.** *Sejam $a \neq 0$ e $b \neq 0$ números naturais, e seja $d = \text{mdc}(a, b)$. Os múltiplos comuns de $a$ e $b$ são os números da forma $\frac{ab}{d}t$ para algum número natural $t$. Em particular $\text{mmc}(a, b) = \frac{ab}{d}$.*

*Demonstração.* Notemos que $\frac{ab}{d}$ é o número natural tal que $\frac{ab}{d}d = ab$, e $\frac{a}{d}$ é o número natural tal que $\frac{a}{d}d = a$. Substituindo a segunda relação na primeira vem $\frac{ab}{d}d = \frac{a}{d}db$, o que implica $\frac{ab}{d} = \frac{a}{d}b$. Portanto $\frac{ab}{d}$ é múltiplo de $b$. Da mesma forma se verifica que $\frac{ab}{d}$ é múltiplo de $a$. Concluímos que todo número da forma $\frac{ab}{d}t$ para algum número natural $t$ é múltiplo comum de $a$ e $b$.

Seja $m$ um múltiplo comum de $a$ e $b$. Existem números naturais $a_1$ e $b_1$ tais que $m = aa_1$ e $m = bb_1$. Portanto $aa_1 = bb_1$. Como $d = \text{mdc}(a, b)$ existem números naturais positivos $a_2$ e $b_2$ tais que $a = da_2$ e $b = db_2$. Por substituição de $a$ e $b$ em $aa_1 = bb_1$ obtemos $da_2a_1 = db_2b_1$. Cancelando $d$ vem $a_2a_1 = b_2b_1$. Vemos assim que $b_2$ é divisor de $a_2a_1$. Em virtude do resultado do Problema 7.3.12 sabemos que $\text{mdc}(a_2, b_2) = 1$. Usando o Teorema 7.3 segue que $b_2$ é divisor de $a_1$. Seja $t$ o número natural tal que $a_1 = b_2t$. Das identidades acima vem $dm = daa_1 = dab_2t = abt$. Por outro lado $\frac{ab}{d}d = ab$. Substituindo essa relação na anterior temos $dm = \frac{ab}{d}dt \Rightarrow m = \frac{ab}{d}t$.

Isso prova que todo múltiplo comum de $a$ e $b$ é da forma $\frac{ab}{d}t$ para algum número natural $t$. O menor valor positivo certamente é assumido para $t = 1$, de modo que $\text{mmc}(a, b) = \frac{ab}{d}$, o que termina a demonstração. □

**Escólio 7.18.** *Sejam $a \neq 0$ e $b \neq 0$ números naturais. Todo múltiplo comum de $a$ e $b$ é múltiplo de $\text{mmc}(a, b)$. Além disso $\text{mmc}(a, b)\,\text{mdc}(a, b) = ab$.*

*Demonstração.* Essas afirmações estão contidas no Teorema acima. □

**Problema resolvido 7.19.** Sejam $a$ e $t$ números naturais positivos. Calcule a quantidade de múltiplos de $t$ no conjunto $\{a, 2a, 3a, \ldots, ta\}$.

*Solução.* A quantidade é $\text{mdc}(a, t)$. Vejamos. Se $j$ é um número natural positivo tal que $ja$ é múltiplo de $t$ então $ja$ é múltiplo comum de $t$ e de $a$, portanto é múltiplo de $\text{mmc}(a, t)$, e é da forma $i\,\text{mmc}(a, t)$ para algum número natural $i$. Reciprocamente todo múltiplo de $\text{mmc}(a, t)$ é também múltipo de $a$, portanto é da forma $ja$ para algum número natural $j$.

Portanto os múltiplos de $t$ no conjunto $\{a, 2a, 3a, \ldots, ta\}$ são os múltiplos de $\text{mmc}(a, t)$ no mesmo conjunto. Vamos listá-los:

$$1 \cdot \text{mmc}(a, t), \quad 2 \cdot \text{mmc}(a, t), \quad 3 \cdot \text{mmc}(a, t), \ldots, i \cdot \text{mmc}(a, t), \ldots$$

Quando $i = \text{mdc}(a, t)$ esse múltiplo é $\text{mdc}(a, t) \cdot \text{mmc}(a, t) = at$, em virtude do Escólio 7.18. Então a lista que queremos é:

$$1 \cdot \text{mmc}(a, t), \quad 2 \cdot \text{mmc}(a, t), \quad 3 \cdot \text{mmc}(a, t), \quad \ldots, \quad \text{mdc}(a, t) \cdot \text{mmc}(a, t) = at.$$

Essa lista tem exatamente $\text{mdc}(a, t)$ elementos e constitui a coleção de todos os mútiplos de $t$ no conjunto dado. □

**Problema resolvido 7.20.** Para todo número natural $n$ a soma $S_n = 1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n}$ forma uma sequência crescente de números reais. É um fato conhecido que esses valores crescem ultrapassando qualquer número dado. Mostre que os valores $S_n$ nunca são números naturais.

*Solução.* Fixado $n$, seja $k$ o maior número natural tal que $2^k \leq n$. Indicamos por $I$ o produto de todos os números ímpares $\leq n$. Dado um número natural $i$ tal que $1 \leq i \leq n$, vejamos como é o produto $I2^{k-1}\frac{1}{i}$. Se for $i = 2^k$, então $I2^{k-1}\frac{1}{i} = I2^{k-1}\frac{1}{2^k} = I\frac{1}{2}$, que não é um número natural, pois $I$ é ímpar. Suponhamos $i \neq 2^k$. Sabemos que $i$ se escreve na forma $i = 2^j m$, sendo $j$ e $m$ números naturais, com $m$ ímpar. Como $i \leq n$ vem $m \leq n$ e então $m$ é um dos fatores do produto $I$. Portanto $I/m$ é um número natural. Ainda $2^j \leq 2^j m \leq n$, portanto $j \leq k$, por definição de $k$. Se $m = 1$ temos $j < k$ pois $i \neq 2^k$. Se $m > 1$ temos $2^j < 2^{j+1} \leq 2^j m \leq n$, portanto $j < k$. Dessa forma $I2^{k-1}\frac{1}{i}$ é um número natural sempre que $i \neq 2^k$. Concluímos que $I2^{k-1}S_n = t + \frac{I}{2}$, para algum número natural $t$. Como $t + \frac{I}{2}$ não é um número natural, segue que $I2^{k-1}S_n$ também não é. Terminamos observando que $S_n$ não é um número natural porque, se fosse, $I2^{k-1}S_n$ também o seria. □

## 7.7 Problemas

**Problema 7.7.1.** Platão, em *As Leis*, comenta propriedades do número 5040, mencionando que ele é múltiplo comum dos números de 1 a 10 e que ele tem 59 divisores não contando com ele mesmo. Verifique as afirmações de Platão. Verifique se 5040 é o menor múltiplo comum dos números de 1 a 10.

**Problema 7.7.2.** Usando a função $\tau(n)$ investigue sob que condições sobre o número natural $n \geq 2$ sua quantidade de divisores positivos é ímpar.

**Problema 7.7.3.** Demonstre que, se $n \geq 2$ é um número natural, escolhendo-se $n+1$ números quaisquer dentre 1, 2, 3, ..., $2n$, existem pelo menos dois dentre os escolhidos tais que um é múltiplo do outro.

**Problema 7.7.4.** Demonstre que se $a$ e $b$ são números naturais relativamente primos e se $ab = m^k$ para números naturais $m$ e $k$, então $a$ e $b$ são potências $k$-ésimas de números naturais.

**Problema 7.7.5.** Encontre condições suficientes de forma que se $a_1 a_2 \ldots a_\ell = m^k$ então todo $a_i$ é uma potência $k$-ésima de um número natural para todo $i$.

**Problema 7.7.6.** Sejam $a \neq 0$ e $b \neq 0$ números naturais relativamente primos. Então $\operatorname{mmc}(a, b) = ab$. Em particular, se $p$ e $q$ são primos diferentes, então $\operatorname{mmc}(p, q) = pq$.

**Problema 7.7.7.** Demonstre que quaisquer que sejam os números naturais $t$, $a$ e $b$ se tem $\operatorname{mmc}(ta, tb) = t \operatorname{mmc}(a, b)$.

**Problema 7.7.8.** Verifique se a fórmula $\operatorname{mmc}(a, b) \operatorname{mdc}(a, b) = ab$ do Escólio 7.18 é válida para três números naturais.

**Problema 7.7.9.** Sejam $a$, $b$ e $c \neq 0$ números naturais tais que $c$ é divisor de $a$ e $b$. Sejam $\frac{a}{c}$ e $\frac{b}{c}$ os quocientes de $a$ por $c$ e de $b$ por $c$, respectivamente. Demonstre que $\operatorname{mdc}(\frac{a}{c}, \frac{b}{c}) = \frac{\operatorname{mdc}(a,b)}{c}$.

**Problema 7.7.10.** Sejam $a \neq 0$ e $b \neq 0$ números naturais. Demonstre que $\frac{\operatorname{mmc}(a,b)}{a}$ e $\frac{\operatorname{mmc}(a,b)}{b}$ são relativamente primos.

**Problema 7.7.11. a)** Sejam $a \neq 0$ e $b \neq 0$ números naturais. Explique por que $\mathcal{M}(a) \cap \mathcal{M}(b) = \mathcal{M}(\operatorname{mmc}(a, b))$. **b)** Mostre que, quaisquer que sejam os números naturais $a_1$, $a_2$, ..., $a_n$ não nulos,

$$\operatorname{mmc}(a_1, a_2, \ldots, a_n) = \operatorname{mmc}(a_1, a_2, \ldots, a_{n-2}, \operatorname{mmc}(a_{n-1}, a_n))$$

**Problema 7.7.12.** Explique por que funciona corretamente o seguinte procedimento para verificar se um dado número natural $10 < p < 10000$ ímpar é ou não primo.

Seja $P$ o produto dos primos ímpares $< 100$. Mais exatamente,

$$P = 115278398197275921237655107366587803 5.$$

Dado $10 < p < 10000$ ímpar, siga as instruções:

*(i)* se $11 \leq p \leq 99$ calcule $d = \text{mdc}(105, p)$;

*(ii)* se $101 \leq p < 10000$ calcule $d = \text{mdc}(P, p)$;

Se $d = 1$, então $p$ é primo. Se $d > 1$ então $p$ é composto.

Esse método é usado em alguns aplicativos computacionais, pois para um computador é relativamente fácil calcular o mdc usando o algoritmo de Euclides.

**Problema 7.7.13.** Sejam $n$ um número natural e $p$ um primo. Mostre que o maior expoente $k$ tal que $p^k$ divide $n!$ é

$$\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \dots$$

Por que essa soma é finita? Essa fórmula vale se $p$ for composto?

## 7.8 Os números perfeitos

Alguns historiadores atribuem aos antigos matemáticos gregos da Escola Pitagórica a observação de que alguns números naturais guardam uma relação especial com seus divisores. Por exemplo,

$$6 = 1 + 2 + 3$$

e

$$28 = 1 + 2 + 4 + 7 + 14$$

são iguais à soma de seus divisores diferentes deles mesmos. Dessa forma foi definida a seguinte classe de números:

**Definição 7.21.** Um número natural chama-se *perfeito* se for igual à soma de seus divisores exceto ele mesmo.

Os antigos matemáticos constataram que não é fácil encontrar números perfeitos. Percebe-se logo que eles são raros. Uma maneira de fazer isso certamente consiste em encontrar uma fórmula que forneça tais números. Quem sabe conseguimos obter uma fórmula examinando os primeiros números perfeitos. A decomposição canônica dos três primeiros números perfeitos é

$$\begin{aligned} 6 &= 2 \cdot 3 \\ 28 &= 2^2 \cdot 7 \\ 496 &= 2^4 \cdot 31 \end{aligned}$$

Vemos que esses números consistem de uma potência de 2 seguida de um número primo, sendo este o antecessor de uma potência de 2. Mais exatamente,

$$\begin{aligned} 6 &= 2^1 \cdot (2^2 - 1) \\ 28 &= 2^2 \cdot (2^3 - 1) \\ 496 &= 2^4 \cdot (2^5 - 1) \end{aligned}$$

Essa lista nos sugere a fórmula $2^{j-1}(2^j - 1)$, sendo $2^j - 1$ um primo. Essa última condição deve ser importante, pois a lista acima não contém o número $2^3(2^4 - 1)$, sendo $2^4 - 1 = 15$, que não é primo.

Essa fórmula para números perfeitos foi observada por Euclides no Livro IX de *Os Elementos*, escrito por volta de 350 a.C. Ele demonstra o

**Teorema 7.22.** *Seja $j \geq 2$ um número natural. Se $2^j - 1$ é primo então $2^{j-1}(2^j - 1)$ é perfeito.*

*Demonstração.* Como $2^j - 1$ é primo, os divisores de $2^{j-1}(2^j - 1)$, exceto ele mesmo, são

$$1 \quad 2 \quad 2^2 \quad \ldots \quad 2^{j-2} \quad 2^{j-1}$$

e

$$2^j - 1 \quad 2(2^j - 1) \quad 2^2(2^j - 1) \quad \ldots \quad 2^{j-2}(2^j - 1)$$

A soma desses números resulta $2^{j-1}(2^j - 1)$, terminando a demonstração. □

Leonard P. Euler, aproximadamente 2000 anos depois de Euclides, demonstrou que todo número perfeito par é da forma $2^{j-1}(2^j - 1)$, com $2^j - 1$ primo, para algum $j \geq 2$.

A fórmula de Euclides para os números perfeitos levou à pesquisa dos números primos da forma $2^j - 1$. Esses números são hoje denominados *números de Mersenne*, em homenagem ao frade Marin Mersenne, que incentivou seu estudo.



Figura 7.1. Marin Mersenne (1588-1648), um padre católico francês, trabalhou em muitas áreas ligadas à Matemática. Desenvolveu as denominadas Leis de Mersenne, que descrevem os harmônicos de uma corda vibrante. Por causa de seu trabalho em Teoria da Música, é conhecido como o pai da acústica. Em Teoria dos Números é reconhecido pelos *primos de Mersenne*, da forma $2^n - 1$, relacionados com os números perfeitos. Ao lado, imagem de Mersenne (mais detalhes na página 261).

## 7.9 Problemas

**Problema 7.9.1.** Observe que um número natural $n$ é perfeito quando $\sigma(n) = 2n$.

**Problema 7.9.2.** Segundo o autor [16], página 219, Nicômano, por volta do ano 100, conhecia os seguintes números perfeitos:

$$P_1 = 6, \quad P_2 = 28, \quad P_3 = 496 \quad \text{e} \quad P_4 = 8128.$$

Verifique que esses números são perfeitos.

**Problema 7.9.3.** Use um aplicativo computacional algébrico para verificar que os números $P_1$, $P_2$, $P_3$ e $P_4$ do Problema 7.9.2 são os únicos números perfeitos $\leq 10\,000$. Se puder estender seus cálculos um pouco mais, verifique que os números perfeitos seguintes são

$$P_5 = 33\,550\,336 \quad \text{e} \quad P_6 = 8\,589\,869\,056.$$

**Problema 7.9.4.** A Escola Pitagórica também considerou outra classe de números especiais, os números amigos. Os números naturais $m$ e $n$ se dizem *amigos* quando a soma dos divisores de $m$, exceto ele mesmo, for igual a $n$, e a soma dos divisores de $n$, exceto ele mesmo, for igual a $m$. Mostre que 220 e 284 são números amigos. Encontre outros pares de números amigos.

## 7.10 Problemas adicionais

**Problema 7.10.1.** Prove que $p > 1$ é primo se e somente se $\text{mdc}((p-1)!, p) = 1$.

**Problema 7.10.2.** Calcule o número natural $n$ sabendo que $8^2 \cdot 55^n$ tem 700 divisores.

**Problema 7.10.3.** Sejam $p$, $q$ e $r$ três primos e $\alpha$, $\beta$, $\gamma$ e $\delta$ números naturais tais que $p^\delta$ é divisor de $p^\alpha q^\beta r^\gamma$. Prove que $\delta \leq \alpha$.

**Problema 7.10.4.** Prove que se $a$, $b \neq 0$ e $c$ são números naturais tais que $b$ é divisor de $c$ então $\text{mdc}(a, b) = \text{mdc}(a + c, b)$.

**Problema 7.10.5.** Demonstre que $\text{mdc}(a, b)$ divide $\text{mdc}(a, bc)$ quaisquer que sejam os números naturais não nulos $a$, $b$ e $c$.

**Problema 7.10.6.** Sejam $a$, $b$ e $n > 0$ números naturais tais que $\text{mdc}(a^n, b^n) = 1$. Ache $\text{mdc}(a, b)$.

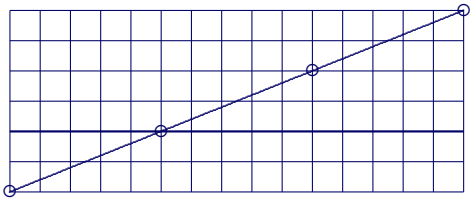
**Problema 7.10.7.** Ao estudar o Tema 5.16.7 talvez você tenha observado as seguintes regularidades: 3 é divisor de $2^2 - 1$, 5 é divisor de $2^4 - 1$, 7 é divisor de $2^6 - 1$, 11 é divisor de $2^{10} - 1$, que sugerem que todo primo $p > 2$ é divisor de $2^{p-1} - 1$. Demonstre essa propriedade, conhecida dos antigos matemáticos chineses.

**Problema 7.10.8.** Demonstre que se $p$ é primo e divide $a^p + b^p$ então $p$ divide $(a+b)^p$, quaisquer que sejam os números naturais $a$ e $b$. Conclua que, nestas condições, $p$ divide $a + b$.

**Problema 7.10.9.** Seja $n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \dots p_s^{e_s}$ a decomposição canônica de $n$, e suponha que exista algum $e_i$ ímpar. Prove que $\sqrt{n}$ não é racional. Conclua que $\sqrt{n}$ é racional se e somente se for um número natural.

**Problema 7.10.10.** Estude e justifique o seguinte método geométrico para calcular o mdc e o mmc. Sejam $a$ e $b$ números naturais não nulos. Consideremos o retângulo de lados $a$ e $b$. Subdividimos o retângulo em $ab$ quadrados unitários e traçamos uma das diagonais do retângulo. Então $\text{mdc}(a, b)$ é a quantidade de vértices de quadrados unitários menos um que a diagonal contém. Para calcular $\text{mmc}(a, b)$, trace um segmento horizontal, ao longo da região retangular, passando por um vértice de quadrado unitário encontrado pela diagonal, o mais próximo de um dos lados horizontais do retângulo. A área do sub-retângulo menor determinado por esse segmento é $\text{mmc}(a, b)$.

A figura abaixo ilustra o caso em que $a = 15$ e $b = 6$. A diagonal passou por 4 vértices de quadrados unitários, portanto $\text{mdc}(15, 6) = 3$. O sub-retângulo tem área $2 \times 15 = 30$, portanto $\text{mmc}(15, 6) = 30$.



**Problema 7.10.11.** Mil armários estão enfileirados e numerados de 1 a 1000 em ordem crescente. Mil estudantes também numerados de 1 a 1000 começam a seguinte brincadeira:

O estudante 1 passa por todos os armários (que inicialmente estavam fechados) e abre suas portas. O estudante 2 passa por todos os armários e inverte as posições das portas dos armários 2, 4, 6, ... O estudante 3 passa por todos os armários e inverte as posições das portas dos armários 3, 6, 9, ... E assim sucessivamente, todos os estudantes passam em ordem por todos os armários e cada um inverte a posição da porta dos armários cujos números são múltiplos de seu próprio número.

Determine quais os números dos armários que ficam abertos após a passagem de todos os estudantes.

**Problema 7.10.12.** Esta é uma demonstração alternativa do Corolário 7.4, que não faz uso de propriedades do mdc. Vi essa demonstração em [63], página 21. O autor a atribui a Alwin R. Korselt. O estudante pode completar os detalhes.

O resultado a ser provado é: Se $p$ é primo e se $p$ é divisor de $ab$ então $p$ é divisor de $a$ ou de $b$, quaisquer que sejam os números naturais $a$ e $b$.

Para demonstrar observemos iniciamente que se $a = 0$ ou $b = 0$ o resultado é verdadeiro. Suponhamos então $a \neq 0$ e $b \neq 0$. Suponhamos que o resultado seja falso, e seja $p$ o menor primo para o qual existem números naturais $a \neq 0$ e $b \neq 0$ tais que $p$ é divisor de $ab$ mas não de $a$ e nem de $b$. Sejam

$$\begin{array}{rcll} a & = & pq_1 + r_1 & 0 < r_1 < p \\ b & = & pq_2 + r_2 & 0 < r_2 < p \end{array} \tag{7.7}$$

Multiplicando essas identidades vemos que $p$ divide $r_1 r_2$, portanto existe um número natural $c$ tal que $r_1 r_2 = pc$. Se fosse $c = 1$ teríamos $r_1 = p$ ou $r_2 = p$, o que não ocorre devido às relações 7.7. Portanto $c > 1$. Ainda de 7.7 temos $c < p$. Consideremos uma decomposição de $c$ como produto de números primos, e seja $p_i$ um primo dessa decomposição. Então $p_i < p$ e $p_i$ é divisor de $r_1 r_2$. Como o resultado é verdadeiro para $p_i$, temos que $p_i$ é divisor de $r_1$ ou de $r_2$. Simplificando $p_i$ na relação $r_1 r_2 = pc$ encontramos números $s_1$ e $s_2$ divisores respectivamente de $r_1$ e $r_2$ tais que $s_1 s_2 = p$. Como $p$ é primo segue que $s_1 = p$ ou $s_2 = p$. Usando novamente 7.7 vem que $p$ é divisor de $a$ ou de $b$, o que é uma contradição.

**Problema 7.10.13.** A seguinte demonstração da unicidade do Teorema Fundamental da Aritmética não faz uso de propriedades do mdc. É devida a Ernst Zermelo, e é de 1912. Vi essa demonstração em [80], página 142. O estudante poderá completar os detalhes.

Suponhamos que, no Teorema Fundamental da Aritmética, a unicidade da decomposição não seja verdadeira. Seja $n > 1$ o menor número natural para o qual isso ocorre. Sejam

$$n = p_1 p_2 \dots p_s = q_1 q_2 \dots q_t$$

decomposições diferentes de $n$ como produto de primos. Podemos escolher a notação de modo que $p_1 \leq p_2 \leq \dots \leq p_s$ e $q_1 \leq q_2 \leq \dots \leq q_t$. É claro que $s > 1$ e $t > 1$. Temos $p_1 \neq q_1$. De fato, se fosse $p_1 = q_1$ existiria um número natural $< n$ com decomposições diferentes. Portanto $p_1 \neq q_1$. Suponhamos $p_1 < q_1$ sem perda de generalidade.

Consideremos o número $m = n - p_1 q_2 q_3 \dots q_t$. Temos $0 < m < n$. Ainda $m = (q_1 - p_1) q_2 q_3 \dots q_t$ e $m = p_1(p_2 \dots p_s - q_2 \dots q_t)$. Portanto $p_1$ é um primo divisor de $m$. Como vale a unicidade da decomposição para $m$, $p_1$ é fator de $q_1 - p_1$, o que é uma contradição.

**Problema 7.10.14.** No Século IX o matemático árabe Thābit ibn Qurrah descobriu uma maneira de gerar números amigos. Sejam $p = 3 \cdot 2^{n-1} - 1$, $q = 3 \cdot 2^n - 1$ e $r = 9 \cdot 2^{2n-1} - 1$

tais que $n > 1$, e $p$, $q$ e $r$ são primos. Então $a = 2^n \cdot p \cdot q$ e $b = 2^n \cdot r$ são amigos. Verifique. Observamos que se trata de uma fórmula interessante, mas limitada, pois não é fácil encontrar números primos dessas formas. Em particular, não se sabe se existem infinitos primos dessas formas.

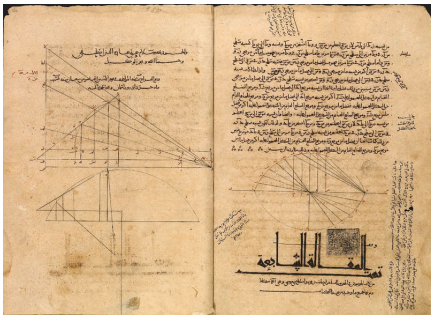


Figura 7.2. Thābit ibn Qurrah foi um impressionante estudioso árabe do Século IX. Contribuiu com a Matemática, Astronomia, Mecânica e Medicina. Em Matemática apresentou muitos resultados em Teoria dos Números, Álgebra e Geometria. Em Astronomia determinou o ano sideral em 365 dias, 6 horas, 9 minutos and 12 segundos (com um erro de 2 segundos). Foi também um grande tradutor para o árabe das obras dos antigos matemáticos gregos. Ao lado, foto de uma página da tradução para o árabe das *Cônicas* de Apolônio de Perga feita por Thābit (mais detalhes na página 261).

## 7.11 Temas para investigação

**Tema 7.11.1.** Seja 97# o produto de todos os primos $\leq 97$. Investigue para quais inteiros $n > 1$ vale a seguinte afirmação:

$$n \text{ é primo} \iff \text{mdc}(97\#, n) = 1.$$

**Tema 7.11.2.** Explique por que o resultado do Problema 7.10.7 pode ser enunciado assim: todo primo $p$ divide $2^p - 2$. Investigue se vale a recíproca: se $n > 1$ é um número natural divisor de $2^n - 2$, então $n$ é primo.

**Tema 7.11.3.** Vimos no Problema 7.10.7 que se $p > 2$ é primo então $p$ é divisor de $2^{p-1} - 1$. Observe que, como $p-1$ é par, $2^{p-1}-1$ pode ser fatorado no produto de $2^{(p-1)/2}+1$ e $2^{(p-1)/2}-1$. Sendo $p$ primo, ele divide pelo menos um desses dois fatores. Investigue sob que condições sobre $p$ se pode afirmar que ele divide o primeiro fator, o mesmo para o segundo. Faça conjecturas.

**Tema 7.11.4.** Investigue sob que condições sobre $n$ o número $2^n + 1$ pode ser primo. Alguma demonstração? E quanto a $a^n + 1$?

**Tema 7.11.5.** Observe os seguintes eventos e faça conjecturas sobre os primos que aparecem. Alguma demonstração?

| | |
|---|---|
| $2^2 + 1 = 5$ | $7^2 + 1 = 50 = 2 \cdot 5 \cdot 5$ |
| $3^2 + 1 = 10 = 2 \cdot 5$ | $8^2 + 1 = 65 = 5 \cdot 13$ |
| $4^2 + 1 = 17$ | $9^2 + 1 = 82 = 2 \cdot 41$ |
| $5^2 + 1 = 26 = 2 \cdot 13$ | $10^2 + 1 = 101$ |
| $6^2 + 1 = 37$ | $11^2 + 1 = 122 = 2 \cdot 61$ |

**Tema 7.11.6.** Vimos no Problema 4.8.25 que as potências quárticas estão nas classes resto zero e resto 1 módulo cinco. Em geral, o que se pode afirmar sobre as $(n-1)$-potências e as classes módulo $n$?

# Capítulo 8

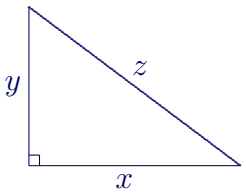
# Os ternos pitagóricos

## 8.1 Introdução

O conhecimento da identidade numérica $3^2 + 4^2 = 5^2$ é de um tempo bastante remoto e sua relação com o triângulo retângulo deu ensejo ao seu uso prático na determinação de ângulos retos em construções arquitetônicas. No mundo antigo essa identidade despertou o interesse dos matemáticos na investigação de métodos que permitissem obter outros números naturais que estão na mesma relação. Posteriormente, no tempo de Euclides, em Alexandria, essa investigação evoluiu para o problema da determinação de todas as soluções de $x^2 + y^2 = z^2$, com $x$, $y$ e $z$ números naturais positivos.

## 8.2 Os ternos pitagóricos

Denominamos *terno*[1] *pitagórico* a qualquer conjunto de números naturais positivos $x$, $y$ e $z$ tais que $x^2 + y^2 = z^2$. A denominação "terno pitagórico" se deve a que, em virtude do Teorema de Pitágoras, a todo terno pitagórico $x$, $y$ e $z$ corresponde um triângulo retângulo com catetos $x$ e $y$ e hipotenusa $z$. Neste texto indicamos os ternos pitagóricos por $(x, y, z)$.



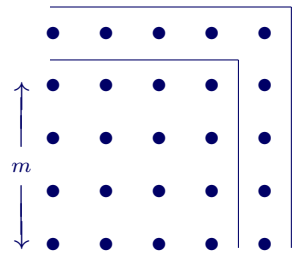

Os antigos matemáticos sumérios conheciam o Teorema de Pitágoras (muito antes de Pitágoras), assim como a relação $3^2+4^2 = 5^2$. Investigavam os números dirigidos por um senso estético que tinha como finalidade a beleza. Sensibilizados pelo impulso de completar o inacabado, eles se perguntaram se existiam outros ternos de números naturais $(x, y, z)$ tais que $x^2 + y^2 = z^2$, e qual a forma de obtê-los. E de fato construíram um método para isso. Podemos facilmente descrever sua metodologia utilizando nossa linguagem algébrica. Tomando um número racional $r \neq 0$ e seu recíproco $r^{-1}$, consideremos o sistema de equações

$$\begin{cases} w + v &= r \\ w - v &= r^{-1} \end{cases} \tag{8.1}$$

[1] Aqui "terno" significa grupo de três números.

A solução desse sistema fornece números racionais $w$ e $v$ tais que $1+v^2 = w^2$. Multiplicando essa identidade por um número natural adequado se obtém um terno pitagórico. Por exemplo, se $r = 5$ obtemos $w = 13/5$ e $v = 12/5$. Multiplicando a identidade $(13/5)^2 = (12/5)^2 + 1$ por $5^2$ vem $13^2 = 12^2 + 5^2$, que fornece o terno pitagórico $(5, 12, 13)$.

Acostumados a identificar números com figuras, os matemáticos da Escola Pitagórica utilizavam o seguinte método para obter ternos pitagóricos. Consideravam um número quadrado da forma $(m+1)^2$, e separavam a figura quadrada correspondente em um quadrado menor com $m^2$ pontos e um gnômon com $2m + 1$ pontos. Portanto $(2m + 1) + m^2 = (m + 1)^2$.




Escolhendo $m$ de modo que $2m+1$ seja um quadrado perfeito, digamos $2m+1 = n^2$, temos $n^2 + m^2 = (m + 1)^2$, o que fornece o terno pitagórico $(n, m, m + 1)$. A figura acima sugere considerar $m = 4$. Então $2m + 1 = 9 = 3^2$, do que resulta $(3, 4, 5)$. Tomando $m = 12$ temos $(5, 12, 13)$.

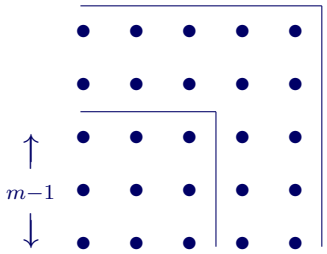
Vamos obter um formato mais adequado para esses ternos pitagóricos. De $2m + 1 = n^2$ temos $m = (n^2 - 1)/2$ e $m + 1 = (n^2 + 1)/2$. Portanto

**Teorema 8.1.** *Qualquer que seja o número natural ímpar $n \geq 3$, são pitagóricos os ternos*

$$\left(n, \frac{n^2-1}{2}, \frac{n^2+1}{2}\right).$$

Eventuais escritos de Pitágoras ou de seus discípulos mais contemporâneos relatando esses assuntos não chegaram até nós, mas Proclus, em seus comentários sobre a história da Matemática, atribui a ele essa descoberta (confira [122], página 8 e [48], página 47).

Método similar era utilizado pela Escola Platônica através de uma modificação do método anterior. Exemplificamos com a figura




em que vemos um quadrado $(m + 1)^2$ repartido em um quadrado menor $(m - 1)^2$ e em dois gnômons com $4m$ pontos. Portanto $4m + (m - 1)^2 = (m + 1)^2$. Se $m$ é um quadrado, digamos $m = n^2$, temos $4m = (2n)^2$ e $(2n)^2 + (m - 1)^2 = (m + 1)^2$. Reescrevendo tudo em função de $n$ temos o

**Teorema 8.2.** *Qualquer que seja o número natural $n \geq 2$, são pitagóricos os ternos*

$$\left(2n, n^2 - 1, n^2 + 1\right).$$

Nenhum desses métodos fornece todos os ternos pitagóricos. O ideal matemático então em construção exigia que se encontrasse uma caracterização completa desses ternos. Procurava-se resolver o seguinte problema:

*Encontrar todas as soluções da equação*

$$x^2 + y^2 = z^2, \quad \text{com } x, y, z \text{ naturais positivos.} \tag{8.2}$$

Não é difícil resolver 8.2. Usando propriedades de figuras geométricas, Euclides, no Livro II de *Os Elementos*, observou a relação

$$ab = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2 \tag{8.3}$$

Portanto, se $a > b$ são números naturais tais que $\sqrt{ab}$, $(a-b)/2$ e $(a+b)/2$ sejam ainda números naturais, então $\big(\sqrt{ab}, (a-b)/2, (a+b)/2\big)$ é um terno pitagórico. Ainda mais, essa fórmula caracteriza os ternos pitagóricos, de acordo com o

**Teorema 8.3** (Euclides)**.** *$(x, y, z)$ é um terno pitagórico se e somente se existem números naturais $a > b$, de mesma paridade, tais que $ab$ é um quadrado perfeito e $(x, y, z) = \big(\sqrt{ab}, (a-b)/2, (a+b)/2\big)$.*

Vejamos uma demonstração detalhada desse teorema. Necessitamos de alguns resultados preliminares.

**Lema 8.4.** *Se $z > y$ são números naturais então $z+y$ e $z-y$ são números naturais de mesma paridade.*

*Demonstração.* De fato, se $y$ e $z$ são ambos pares ou ambos ímpares, sua soma e sua diferença são pares. Por outro lado, se $y$ for par e $z$ for ímpar, ou o contrário, sua soma e sua diferença são ímpares. Portanto $z+y$ e $z-y$ são números naturais de mesma paridade. □

**Lema 8.5.** *Se os números naturais $a$ e $b$ têm a mesma paridade, então $(a+b)/2$ é um número natural. Se também ocorrer que $a > b$, então $(a-b)/2$ é número natural.*

Esses resultados não valem se os números $a$ e $b$ têm paridade oposta. Por exemplo, $(9+8)/2 = 17/2$ e $(9-8)/2 = 1/2$ não são números naturais.

*Demonstração.* A soma e a diferença de pares é par, assim como a soma e a diferença de ímpares. Portanto $(a+b)/2$ e $(a-b)/2$ são números naturais. □

*Demonstração do Teorema 8.3* Seja $(x, y, z)$ um terno pitagórico. Então $x$, $y$ e $z$ são números naturais tais que $x^2+y^2 = z^2$. Podemos escrever $x^2 = z^2 - y^2 = (z+y)(z-y)$. Sejam $a = z+y$ e $b = z-y$. Como $z > y$ então $a$ e $b$ são números naturais tais que $a > b$, e como $x^2 = ab$ segue que $ab$ é um quadrado perfeito. Temos ainda que $a$ e $b$ têm a mesma paridade (Lema 8.4). Resolvendo o sistema $a = z+y$ e $b = z-y$ em $y$ e $z$ obtemos $y = (a-b)/2$ e $z = (a+b)/2$. Portanto $(x, y, z) = (\sqrt{ab}, (a-b)/2, (a+b)/2)$.

Reciprocamente, sejam $a > b$ números naturais de mesma paridade tais que $ab$ é um quadrado perfeito. Seja $(x, y, z) = (\sqrt{ab}, (a-b)/2, (a+b)/2)$. Pelo fato de $a$ e $b$ terem a mesma paridade, $z = (a+b)/2$ e $y = (a-b)/2$ são números naturais (Lema 8.5). Pelo fato de $ab$ ser um quadrado perfeito, $x = \sqrt{ab}$ é um número natural. Calculando $x^2 + y^2$ obtemos $z^2$, do que resulta que $(x, y, z)$ é um terno pitagórico. □

## 8.3 Problemas

**Problema 8.3.1.** Demonstre que se $(x, y, z)$ é um terno pitagórico então existe um triângulo retângulo com catetos $x$ e $y$ e hipotenusa $z$.

**Problema 8.3.2.** Encontre todas as soluções de 8.3 supondo que pelo menos um dos números $x$, $y$ ou $z$ seja igual a zero.

**Problema 8.3.3.** **a)** Resolva o sistema 8.1 descrito na página 183 e verifique que sua solução fornece números racionais $w$ e $v$ tais que $1 + v^2 = w^2$. **b)** Tomando $r = 12/5$, use esse método para obter um terno de números pitagóricos. Encontre outros exemplos numéricos. **c)** Tomando $r = n$, sendo $n$ um número natural, encontre uma fórmula que fornece infinitos ternos pitagóricos. **d)** O que acontece se $r = m/n$ ?

**Problema 8.3.4.** **a)** Demonstre os teoremas 8.1 e 8.2. **b)** Verifique que aquelas fórmulas, mesmo tomadas conjuntamente, não fornecem todos os ternos pitagóricos.

**Problema 8.3.5.** Segundo [122] página 9, na antiga Índia se usava o seguinte método para obter ternos pitagóricos. Escrevendo $x^2+y^2 = z^2$ na forma $x^2 = z^2-y^2$ temos $x^2 = (z+y)(z-y)$. Impondo uma condição adequada para $z-y$, por exemplo $z-y = 1$, e tomando um valor ímpar $\geq 3$ para $x$, digamos, $x = 5$, resolvemos o sistema $z - y = 1$ e $z + y = 25$ e obtemos $y = 12$ e $z = 13$. Isso nos dá o terno pitagórico $(5, 12, 13)$. **a)** Confirme as afirmações acima. **b)** Encontre outros ternos pitagóricos usando outros valores para $x$, por exemplo, $x = 3$, $x = 7$, etc. Por que $x$ deve ser ímpar? **c)** Tomando $x = n$, sendo $n \geq 3$ um número natural, encontre uma fórmula geral para se obter ternos pitagóricos. **d)** O que ocorre se considerarmos $z-y = 2$?

**Problema 8.3.6.** Utilize o Teorema 8.3 para obter exemplos de ternos pitagóricos.

**Problema 8.3.7.** O autor [122], na página 7, descreve que uma antiga regra chinesa para o cômputo de números pitagóricos é equivalente a $(x, y, z) = (mn, (m^2 - n^2)/2, (m^2 + n^2)/2)$, sendo $m > n > 0$ números naturais de mesma paridade. **a)** Confirme que essa regra realmente fornece ternos pitagóricos. **b)** Encontre ternos pitagóricos usando essa regra. **c)** Mostre que essa regra não fornece todos os ternos pitagóricos. **d)** Deduza a antiga regra chinesa introduzindo os valores $x = mn$ e $z - y = n^2$ em $x^2 + y^2 = z^2$.

## 8.4 Ternos pitagóricos, o estado da arte

O problema da caracterização dos ternos pitagóricos tem outra solução, mais elegante do que a dada no Teorema 8.3. Para apresentá-la ao estudante necessitamos de alguns resultados iniciais.

Observamos inicialmente que um terno pitagórico qualquer gera outros infinitos ternos mediante multiplicação por um número natural positivo. Por exemplo, multiplicando $(3, 4, 5)$ por 2 obtemos o terno $(6, 8, 10)$. Em geral, se $(x, y, z)$ é um terno pitagórico e $k > 0$ é um número natural, então $(kx, ky, kz)$ também é um terno pitagórico. De fato, $(kx)^2+(ky)^2 = k^2(x^2+y^2) = k^2z^2 = (kz)^2$.

Reciprocamente, dado um terno pitagórico $(x, y, z)$, podemos eventualmente reduzi-lo a outro menor dividindo seus termos por algum divisor comum. Por exemplo, dividindo o terno pitagórico $(32, 60, 68)$ por 2 obtemos $(16, 60, 68)$, e por 4 obtemos $(8, 15, 17)$. Esse último não se reduz mais, pois $\text{mdc}(8, 15, 17) = 1$, e assim 8, 15 e 16 não têm divisor comum $> 1$.

Em geral, dado um terno pitagórico $(x, y, z)$, seja $d = \text{mdc}(x, y, z)$. Podemos escrever $x = dx_1$, $y = dy_1$ e $z = dz_1$, sendo $x_1$, $y_1$ e $z_1$ números naturais positivos. Então $(x_1, y_1, z_1)$ também é um terno pitagórico. De fato, $x^2 + y^2 = z^2 \Rightarrow (dx_1)^2 + (dy_1)^2 = (dz_1)^2$. Podemos cancelar $d > 0$ e assim $x_1^2 + y_1^2 = z_1^2$.

Fica claro que para caracterizar os ternos pitagóricos basta determinar aqueles que estão na forma mais reduzida, pois todos os outros deles derivam.

**Definição 8.6.** Um terno pitagórico $(x, y, z)$ diz-se *primitivo* quando $x$, $y$ e $z$ são relativamente primos, ou seja, se $\text{mdc}(x, y, z) = 1$.

Dados números naturais positivos $x$, $y$ e $z$, seja $d$ seu maior divisor comum. Então $x/d$, $y/d$ e $z/d$ são números naturais relativamente primos. De fato, em virtude do resultado do Problema 7.3.3 temos $d\,\text{mdc}(x/d, y/d, z/d) = \text{mdc}(d(x/d), d(y/d), d(z/d)) = d$. Cancelando $d$ vem $\text{mdc}(x/d, y/d, z/d) = 1$.

Portanto, se $(x, y, z)$ é um terno pitagórico, então $(x/d, y/d, z/d)$ é um terno pitagórico primitivo.

**Lema 8.7.** *Se $(x, y, z)$ é um terno pitagórico, então $x$ e $y$ não podem ser ambos ímpares.*

*Demonstração.* Suponhamos que o sejam. Então existem números naturais $p$ e $q$ tais que $x = 2p+1$ e $y = 2q+1$. Segue que $z^2 = x^2 + y^2 = (2p+1)^2 + (2q+1)^2 = 4t+2$, para um certo número natural $t$. Temos assim duas informações sobre $z^2$: é par e não tem 4 como fator. Mas isso não é possível. De fato, como $z^2$ é par, temos que $z$ é par. Então podemos escrever $z = 2s$ para algum número natural $s$. Segue que $z^2 = (2s)^2 = 4s^2$, e $z^2$ tem 4 como fator, o que é uma contradição. Essa contradição se originou do fato de supormos $x$ e $y$ ambos ímpares. □

**Lema 8.8.** *Se $(x, y, z)$ é um terno pitagórico primitivo, então $x$ e $y$ têm paridade oposta.*

*Demonstração.* Já vimos que $x$ e $y$ não podem ser ambos ímpares. Se $x$ e $y$ são pares, da relação $x^2 + y^2 = z^2$ segue que $z$ também é par, contrariando a hipótese de ser $(x, y, z)$ um terno pitagórico primitivo. Concluímos que $x$ e $y$ têm paridade oposta. □

Se $m > n > 0$ são números naturais, considerando $r = m/n$ no método sumério 8.1, obtemos os ternos pitagóricos $(2mn, m^2 - n^2, m^2 + n^2)$ (confira o Problema 8.3.3). Essa é a fórmula adotada no

**Teorema 8.9.** *$(x, y, z)$ é um terno pitagórico primitivo com $x$ par se e somente se existem números naturais $a > b > 0$ de paridade oposta e relativamente primos tais que*

$$(x, y, z) = (2ab,\ a^2 - b^2,\ a^2 + b^2).$$

*Demonstração.* Seja $(x, y, z)$ um terno pitagórico primitivo com $x$ par. Em virtude do Lema 8.8 $y$ é ímpar. De $x^2 + y^2 = z^2$ temos $z$ ímpar, $z > y$ e $x^2 = z^2 - y^2 = (z + y)(z - y)$. Notemos que $z + y$ e $z - y$ são pares, portanto podemos considerar os números naturais $a_1 = (z + y)/2$ e $b_1 = (z - y)/2$. Temos $(x/2)^2 = a_1 b_1$. Afirmamos que $\text{mdc}(a_1, b_1) = 1$. De fato, se existe um primo $p$ divisor de $a_1$ e $b_1$, então $p$ divide $a_1 + b_1 = z$ e $a_1 - b_1 = y$. Da relação $x^2 + y^2 = z^2$ segue que $p$ divide $x$, o que não é possível, pois $(x, y, z)$ é um terno pitagórico primitivo. Portanto $\text{mdc}(a_1, b_1) = 1$. Aplicando o resultado do Teorema 7.11 sabemos que nestas condições $a_1$ e $b_1$ são quadrados perfeitos. Sejam $a$ e $b$ números naturais tais que $a_1 = a^2$ e $b_1 = b^2$. Temos $(x, y, z) = (2ab,\ a^2 - b^2,\ a^2 + b^2)$ e é claro que $a > b > 0$ e $\text{mdc}(a, b) = 1$. Ainda, se $a$ e $b$ tivessem a mesma paridade, $x$, $y$ e $z$ seriam pares, contrariando o fato de que $(x, y, z)$ é primitivo. Portanto $a$ e $b$ têm paridade oposta, e terminamos a primeira parte da demonstração.

Reciprocamente sejam $a > b$ números naturais de paridade oposta e relativamente primos. Seja $(x, y, z) = (2ab, a^2 - b^2, a^2 + b^2)$. É claro que $x$ é par e $y$ é ímpar. Ainda $(x, y, z)$ é um terno pitagórico pois $x^2 + y^2 = (2ab)^2 + (a^2 - b^2)^2 = 4a^2b^2 + a^4 - 2a^2b^2 + b^4 = a^4 + 2a^2b^2 + b^4 = (a^2 + b^2)^2 = z^2$. Falta mostrar que $(x, y, z)$ é primitivo. Suponhamos que exista $p$ primo divisor de $x$, $y$ e $z$. Como $y$ é ímpar temos $p \neq 2$. Ainda $p$ divide $y + z = 2a^2$, portanto $p$ divide $a$, e $p$ divide $z - y = 2b^2$, logo $p$ divide $b$. Mas isso não é possível, pois $a$ e $b$ são relativamente primos. Portanto não existe primo divisor de $x$, $y$ e $z$, e $\text{mdc}(x, y, z) = 1$. □

**Corolário 8.10.** *Todos os ternos pitagóricos $(x, y, z)$ são dados, sem repetição, pela fórmula*

$$(x, y, z) = (2abt,\ (a^2 - b^2)t,\ (a^2 + b^2)t)$$

*(trocando $x$ por $y$ se necessário) sendo $a > b > 0$ números naturais de paridade oposta e relativamente primos, e $t$ qualquer número natural positivo.*

*Demonstração.* Se $a > b > 0$ e $t > 0$ são números naturais e se $x$, $y$ e $z$ são dados por $x = 2abt$, $y = (a^2 - b^2)t$ e $z = (a^2 + b^2)t$, é fácil verificar que $x^2 + y^2 = z^2$, e portanto $(x, y, z)$ é um terno pitagórico. Reciprocamente, dado um terno pitagórico $(x, y, z)$, seja $t = \text{mdc}(x, y, z)$. Então $(x/t, y/t, z/t)$ é um terno pitagórico primitivo. Trocando $x$ por $y$ se necessário, podemos supor que $x/t$ é par e $y/t$, ímpar. O Teorema 8.9 garante que existem números naturais $a > b > 0$ de paridade oposta e relativamente primos tais que $x/t = 2ab$, $y/t = a^2 - b^2$ e $z/t = a^2 + b^2$. Portanto $(x, y, z) = (2abt, (a^2 - b^2)t, (a^2 + b^2)t)$ tem a forma requerida.

Para terminar a demonstração falta provar que a fórmula dada fornece ternos pitagóricos sem repetição. Essa observação é atribuída em [28], página 169, a Leopold Kronecker. Sejam $(x, y, z) = (2abt, (a^2 - b^2)t, (a^2 + b^2)t)$ e $(x, y, z) = (2a_1b_1t_1, (a_1^2 - b_1^2)t_1, (a_1^2 + b_1^2)t_1)$ com as condições do enunciado do Corolário. Queremos demonstrar que $a = a_1$, $b = b_1$ e $t = t_1$. Começamos observando que $t = \text{mdc}(x, y, z)$. De fato, $t$ é um divisor comum de $x$, $y$ e $z$. Como $a$ e $b$ são relativamente primos, $a^2 - b^2$ e $a^2 + b^2$ são relativamente primos, portanto $t$ é o maior divisor comum de $y$ e $z$, e assim $t$ é o maior divisor comum de $x$, $y$ e $z$. Da mesma forma $t_1 = \text{mdc}(x, y, z)$, o que implica $t = t_1$. Como $y + z = (a^2 - b^2)t + (a^2 + b^2)t = 2a^2t$ e $y + z = (a_1^2 - b_1^2)t + (a_1^2 + b_1^2)t = 2a_1^2t$, segue que $2a^2t = 2a_1^2t$ o que implica $a = a_1$. Temos também $b = b_1$, o que termina a demonstração. □

## 8.5 Problemas

**Problema 8.5.1.** Obtenha exemplos de ternos pitagóricos primitivos usando a fórmula do Teorema 8.9.

**Problema 8.5.2.** Obtenha todos os ternos pitagóricos em que um dos números é 16.

**Problema 8.5.3.** Demonstre que se $x$, $y$ e $z$ são números naturais tais que $x^2 + y^2 = z^2$ então $x$ ou $y$ é múltiplo de 3 e $xy$ é múltiplo de 6.

**Problema 8.5.4.** Demonstre que se $x$, $y$ e $z$ são números naturais tais que $x^2 + y^2 = z^2$ então 5 divide um dos números $x$, $y$ ou $z$.

**Problema 8.5.5.** Dado um número natural $c$, prove que existem números naturais $a$ e $b$ tais que $a^2 - b^2 = c$ se e somente se existem números naturais $m$ e $n$, de mesma paridade, tais que $c = mn$.

## 8.6 Pierre de Fermat e seu último teorema

Pierre de Fermat nasceu na França, provavelmente em 1601, e era advogado e conselheiro do Parlamento de Toulouse. Matemático amador nas horas vagas, distinguiu-se por importantes contribuições, principalmente em Teoria dos Números. Fermat publicava muito pouco e suas descobertas eram conhecidas graças à sua correspondência com outros estudiosos, um costume da época. Durante um certo tempo Fermat estudou a versão latina do livro *Arithmetica*, escrito pelo matemático grego Diofanto de Alexandria no Século III. Nas margens desse livro Fermat fazia anotações inspiradas nos estudos de Diofanto, enunciando teoremas sem apresentar demonstrações. Fermat faleceu em 1665, e após sua morte essas anotações foram publicadas por um de seus filhos. Os teoremas propostos por Fermat foram demonstrados por matemáticos que viveram logo após ele, particularmente por Leonard P. Euler, no Século XVIII. Entretanto um desses teoremas enunciados por Fermat resistiu às tentativas de demonstração por aproximadamente 350 anos. Ficou conhecido como o *Último Teorema de Fermat*.

Às margens de seu exemplar de *Arithmetica*, e ao lado de um estudo de Diofanto sobre os ternos pitagóricos, escreveu Fermat as palavras que se tornariam famosas: *Dividir um cubo em dois cubos, uma quarta potência em duas quartas potências, e em geral uma potência acima da quadrada em duas do mesmo tipo, é impossível: encontrei uma demonstração maravilhosa desse fato. Esta margem é muito pequena para contê-la.*[2]

Em outros termos, Fermat enunciou o seguinte

**Teorema 8.11.** *Para todo número natural $n \geq 3$ não existe solução para a equação*

$$x^n + y^n = z^n, \quad \textit{com } x, y, z \textit{ naturais positivos.} \tag{8.4}$$

A demonstração desse resultado é bastante complicada e utiliza técnicas algébricas avançadas. Nesses três séculos e meio inúmeros matemáticos contribuíram com idéias e técnicas, quando foi finalmente finalizado por Andrew Wiles em 1994. Quanto à demonstração anunciada por Fermat, a maioria dos historiadores, senão todos, acreditam que ele se enganou.



Figura 8.1. Pierre de Fermat era matemático (amador, como já dissemos), advogado, juiz, jurista e poliglota. Juntamente com René Descartes, inventou a Geometria Analítica. Deu uma contribuição significativa à Probabilidade e ao Cálculo Infinitesimal. É considerado o criador da moderna Teoria dos Números, tendo seu nome ligado, por exemplo, aos números de Fermat $2^{2^n}+1$ e ao Pequeno Teorema de Fermat (além do Último Teorema de Fermat). Ao lado, foto de monumento a Pierre de Fermat (mais detalhes na página 261).

## 8.7 Problemas adicionais

**Problema 8.7.1.** Vimos no Problema 6.6.4 que se 3 divide $a^2 + b^2$ então 3 divide $a$ e $b$, quaisquer que sejam os números naturais $a$ e $b$. Use isso para provar que se $(x, y, z)$ é um terno pitagórico primitivo então 3 não é divisor de $z$.

[2]Tradução livre do original em latim, [3], página 40.

**Problema 8.7.2.** Demonstre que, quaisquer que sejam os números naturais $a$ e $b$, $a^2+b^2$ nunca é da forma $4k+3$, para qualquer número natural $k$. Use isso para provar que se $(x, y, z)$ é um terno pitagórico primitivo então $z$ é da forma $4k+1$, para algum número natural $k$.

**Problema 8.7.3.** Seja $n$ um número natural ímpar. Prove que $n$ é composto se e somente se a equação

$$x^2 - y^2 = n, \quad x, y \in \mathbb{N}$$

tem mais de uma solução.

**Problema 8.7.4.** Complete os detalhes desta demonstração do Teorema 8.9, atribuída a Euler ([28], página 167). Seja $(x, y, z)$ um terno pitagórico primitivo, com $x$ par. Seja $\frac{z-y}{x} = \frac{b}{a}$, com $a > b > 0$ relativamente primos. Substituindo $z = y+x\frac{b}{a}$ em $z^2 = x^2+y^2$ vem $2aby = (a^2-b^2)x$. Então $a$ e $b$ têm paridade oposta e $2ab$ e $a^2-b^2$ são relativamente primos. Portanto $2ab$ é divisor de $x$ e $a^2 - b^2$ é divisor de $y$. Sejam $x = 2abl$ e $y = (a^2 - b^2)k$. Segue $l = k$ e $z = (a^2 + b^2)l$. Como $\text{mdc}(x, y, z) = 1$ vem $l = 1$.

## 8.8 Tema para investigação

**Tema 8.8.1.** Um triângulo cujos lados são números naturais e cuja área é também um número natural chama-se *triângulo heroniano*, em homenagem a Heron de Alexandria, matemático grego que viveu no primeiro século de nossa era. Chamamos de *triângulo pitagórico* a todo triângulo retângulo cujos lados são números naturais. **a)** Explique por que os triângulos pitagóricos correspondem às soluções positivas de $x^2 + y^2 = z^2$. **b)** Demonstre que todo triângulo pitagórico é heroniano. **c)** Dê exemplos de triângulos heronianos que não são pitagóricos. **d)** Verifique se existem infinitos triângulos heronianos.

# Parte III

# Introdução à teoria dos números inteiros

# Capítulo 9

# Os números inteiros

## 9.1 Introdução

Vimos, no Capítulo 1, que o homem, usando sua capacidade de abstração, constrói o conceito de número natural, visando, inicialmente, a contagem de objetos discretos. Obtém dessa forma os números 1, $1+1$, $1+1+1$, ... No Capítulo 4, seção 4.5, introduzimos o conceito de zero como número natural, e definimos o conjunto $\mathbb{N}$ dos números naturais por

$$\mathbb{N} = \{0, 1, 2, 3, 4, \ldots\}$$

No presente capítulo estudamos os números inteiros como uma extensão desse conjunto.

## 9.2 A qualidade dos números negativos

Todo número natural tem um aspecto quantitativo, pois mede a quantidade de elementos de um conjunto. Mas esse número também traz uma idéia qualitativa, que é a positividade. Assim, ao dizer "5 livros", traduzimos uma afirmação positiva sobre essa específica quantidade de livros. Mas a experiência nos leva à necessidade de considerar números naturais com a qualidade de negativo. Podemos fazer isso com uma construção do tipo "faltam-me 5 livros", ou então "a temperatura está 8 graus abaixo de zero". A Álgebra também apresenta situações em que se faz necessário considerar os números naturais com a qualidade de negatividade. Por exemplo, ao procurar uma possível solução $x$ da equação $7+x=3$, vemos que nenhum número natural pode exercer esse papel. Percebemos que o valor quantitativo de $x$ deve ser 4, mas $x$ deve agir na operação $7+x$ de forma oposta à adição usual. É necessário que $+x$ opere retirando quatro unidades de 7, para resultar 3.

Essas observações nos trazem a ideia de considerar, para cada número natural $n \neq 0$, um outro número, quantitativamente igual a $n$ mas de qualidade oposta. Chamamos de *negativos* a esses números.

Convém criar uma notação para esse novo número, por exemplo, $\tilde{n}$. Vemos que $\tilde{n}$ deve ser caracterizado pelas relações

$$n + \tilde{n} = 0 = \tilde{n} + n \tag{9.1}$$

para todo número natural $n \in \mathbb{N}$.

Em particular, com a construção desses números, poderemos dizer que a solução da equação $7+x=3$ dada acima passaria a ser $x = \tilde{4}$, pois $7+\tilde{4} = (3+4)+\tilde{4} = 3+(4+\tilde{4}) = 3+0 = 3$.

O estudante bem sabe que a Matemática consagrou a notação $-n$ para o número negativo correspondente a $n$. Dizemos que $-n$ é o *oposto* de $n$.

Existem razões práticas para a escolha da notação $-n$ para o oposto de $n$. Ela simplifica a manipulação de expressões algébricas, combinando a notação de subtração com a de oposto. Por exemplo, a adição de 8 com $-5$, a ser representada por $8+(-5)$, poderá ser simplificada para $8-5$, pois ambas as expressões têm o mesmo significado: estão sendo retiradas 5 unidades de 8.

Observamos que a consideração dos números negativos não constitui uma mera substituição da subtração. No contexto dos números naturais a subtração $a-b$ só tem sentido quando $a \geq b$. No novo contexto, com o acréscimo dos números negativos, podemos processar a subtração $a-b$ quaisquer que sejam o números naturais $a$ e $b$. Se $b > a$ o valor de $a-b$ será um desses números negativos, mais exatamente, o oposto de $b-a$.

Poderíamos continuar a construção dos números inteiros usando os métodos com os quais os professores os ensinam para os estudantes da escola básica. Mas neste curso, como já estamos em uma fase mais adiantada em nosso caminho para a álgebra abstrata, preferimos proceder com um grau um pouco maior de formalidade. É o que fazemos na seção seguinte.

## 9.3 O conjunto dos números inteiros

Dado o conjunto dos números naturais $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$, para todo número natural $n \neq 0$ consideramos o símbolo $-n$. Definimos

**Definição 9.1.** O *conjunto dos números inteiros* é

$$\mathbb{Z} = \{\ldots -3, -2, -1, 0, 1, 2, 3, \ldots\} \tag{9.2}$$

Em outros termos, $\mathbb{Z} = \mathbb{N} \cup \{\ldots -3, -2, -1\}$. Conforme já mencionamos, para todo número natural $n \neq 0$ o número $-n$ é denominado *oposto* de $n$. O elementos do conjunto $\mathbb{Z}_+ = \{1, 2, 3, \ldots\}$ são denominados *inteiros positivos*, e os do conjunto $\mathbb{Z}_- = \{\ldots -3, -2, -1\}$, *inteiros negativos*. Se não quisermos usar mais o símbolo $\mathbb{N}$, uma forma é substituí-lo por $\mathbb{Z}_+ \cup \{0\}$.

Obtemos assim um novo conjunto de números que inclui os números naturais. Esperamos que esse novo conjunto tenha maiores possibilidades do que o conjunto $\mathbb{N}$.

O símbolo $-n$ foi definido para o caso em que $n$ é um número natural. Completamos nossa definição escrevendo $-(-n) = n$ para todo $n \in \mathbb{N}$, de modo que o símbolo $-n$ agora fica definido também para o caso em que $n$ é inteiro negativo. Nesse caso dizemos que $-n$ tem $n$ como oposto.

Valem as relações

$$a + (-a) = 0 = (-a) + a \tag{9.3}$$

para todo número inteiro $a \in \mathbb{Z}$.

Nossa primeira providência é estender para $\mathbb{Z}$ os conceitos de adição e multiplicação já definidos em $\mathbb{N}$. A subtração também é definida mais abaixo, e a divisão será estudada na Seção 9.7.

A adição e a multiplicação de inteiros podem ser definidas pela lista de condições apresentadas a seguir, levando-se em conta que já estão definidas para números naturais. O símbolo $-0$ pode eventualmente aparecer. Nesse caso entendemos que $-0 = 0$.

**Definição 9.2.** Dados $m, n \in \mathbb{N}$, supomos, sem perda de generalidade, que $m \geq n$. Seja $k \in \mathbb{N}$ tal que $m = n + k$. Definimos:

**(i)** $m + (-n) = (-n) + m = k$;

**(ii)** $(-m) + n = n + (-m) = -k$;

**(iii)** $(-m) + (-n) = -(m + n) = (-n) + (-m)$;

**(iv)** $(-m)n = n(-m) = -(mn)$;

**(v)** $(-m)(-n) = mn = (-n)(-m)$.

O estudante pode verificar que as condições (i), (ii) e (iii) definem a soma $a + b$ para os todos os casos em que $a$ ou $b$ não são números naturais, e igualmente as condições (iv) e (v) definem o produto $ab$. Pode ser útil examinar exemplos com todas as possibilidades. Para ver o que é $4 + (-7)$, escrevemos $m = 7$ e $n = 4$. Então $k = m - n = 7 - 4 = 3$. Usando a segunda identidade do item (ii) da Definição, temos $4 + (-7) = n + (-m) = -k = -3$.

As propriedades comutativa da adição e da multiplicação em $\mathbb{Z}$ podem ser facilmente verificadas. Como exemplo, vamos provar que $a + b = b + a$ para o caso em que $a$ é positivo e $b$ é negativo. Seja $b = -t$, para $t$ positivo. Se $a \geq t$ escrevemos $a = m$ e $t = n$. Usando a condição (i) acima vem $a + b = m + (-n) = (-n) + m = b + a$. Se $t > a$ escrevemos $t = m$ e $a = n$. Usando a condição (ii) acima vem $a + b = n + (-m) = (-m) + n = b + a$.

A propriedade associativa da adição em $\mathbb{Z}$ está praticamente verificada no Problema Resolvido 9.6 apresentado abaixo. O estudante está convidado a verificar a propriedade associativa da multiplicação em $\mathbb{Z}$, assim como a distributiva.

A relação de ordem natural já considerada em $\mathbb{N}$ pode se estender para $\mathbb{Z}$ da seguinte forma:

**Definição 9.3.** Dados $a, b \in \mathbb{Z}$, escrevemos $a < b$ quando $b + (-a) \in \mathbb{Z}_+$.

Os símbolos $>$ $\leq$ $\geq$ são definidos de modo análogo ao que foi feito na Seção 3.4.

Nos Problemas 9.4 solicitamos do estudante a demonstração de várias propriedades relacionadas com a ordem em $\mathbb{Z}$.

A seguir definimos a operação de subtração em $\mathbb{Z}$:

**Definição 9.4.** Dados $a, b \in \mathbb{Z}$, a *diferença* $a - b$ é definida por $a - b = a + (-b)$.

Todo $n \in \mathbb{Z}$ e seu oposto $-n$ têm o mesmo valor quantitativo. A esse valor comum denominamos *valor absoluto*. Mais exatamente, temos a

**Definição 9.5.** Dado $m \in \mathbb{Z}$, seu *valor absoluto* é anotado por $|m|$ e definido por

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

**Problema resolvido 9.6.** Demonstre a propriedade associativa da adição em $\mathbb{Z}$. Isto é, $(a + b) + c = a + (b + c)$ quaisquer que sejam $a, b, c \in \mathbb{Z}$.

*Solução.* Examinemos oito casos, conforme cada um dos números $a$, $b$ ou $c$ esteja ou não em $\mathbb{N}$.

*1º caso* Se $a, b, c \in \mathbb{N}$ já temos $(a + b) + c = a + (b + c)$, conforme foi observado na Seção .

*2º caso* Suponhamos $a, b \in \mathbb{N}$ mas $c \notin \mathbb{N}$. Seja $c = -t$, com $t \in \mathbb{N}$. Temos duas possibilidades: $b \geq t$ ou $b < t$. Se $b \geq t$ escrevemos $b = t + k$. Temos também $a + b \geq t$ e $a + b = t + a + k$. Portanto

$$a + (b + c) = a + [b + (-t)] = a + k$$

e

$$(a+b)+c=(a+b)+(-t)=a+k$$

em virtude do item (i) de 9.2. Portanto $(a+b)+c=a+(b+c)$.

Suponhamos agora que $b<t$. Escrevemos $t=b+k$. Então

$$a+(b+c)=a+[b+(-t)]=a+(-k)$$

em virtude do item (ii) de 9.2. Comparando $a+b$ com $t$ temos dois subcasos. Suponhamos primeiro que $a+b<t$. Seja $t=a+b+l$. Juntando isso com $t=b+k$ vem $a+l=k$ (em $\mathbb{N}$ vale a Lei do Cancelamento da adição). Em virtude dos itens (i) e (ii) de 9.2 vem

$$a+(-k)=-l \quad \text{e} \quad (a+b)+c=(a+b)+(-t)=-l.$$

Considerando que $a+(b+c)=a+(-k)$ segue $(a+b)+c=a+(b+c)$.

Suponhamos agora $a+b\geq t$. Seja $a+b=t+l$. Juntando isso com $t=b+k$ vem $a=k+l$. Portanto

$$a+(-k)=l \quad \text{e} \quad (a+b)+c=(a+b)+(-t)=l.$$

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

*3º caso* Suponhamos $a\in\mathbb{N}$ mas $b,c\notin\mathbb{N}$.

A demonstração é análoga à do 2º caso.

*4º caso* Suponhamos $a,b,c\notin\mathbb{N}$.

Sejam $a=-u$, $b=-s$ e $c=-t$. Aplicando o item (iii) de 9.2 temos $(a+b)+c=[(-u)+(-s)]+(-t)=-(u+s)+(-t)=-[(u+s)+t]=-[u+(s+t)]=(-u)+[-(s+t)]=(-u)+[(-s)+(-t)]=a+(b+c)$.

*5º caso* Suponhamos $a,b\notin\mathbb{N}$ e $c\in\mathbb{N}$. Simétrica ao 3º caso.

*6º caso* Suponhamos $a\notin\mathbb{N}$ e $b,c\in\mathbb{N}$. Simétrica ao 2º caso.

*7º caso* Suponhamos $a,c\notin\mathbb{N}$ e $b\in\mathbb{N}$. Trocando $a$ e $b$, este é o 3º caso.

*8º caso* Suponhamos $b\notin\mathbb{N}$ e $a,c\in\mathbb{N}$. Trocando $b$ e $c$, este é o 2º caso. □

## 9.4 Problemas

**Problema 9.4.1.** Verifique que as condições (i), (ii) e (iii) da Definição 9.2 definem a soma $a+b$ para os casos em que $a$ ou $b$ são números inteiros negativos. Verifique ainda que as condições (iv) e (v) da mesma Definição definem o produto $ab$ para os casos em que $a$ ou $b$ são números inteiros negativos.

*Solução para a multiplicação.*

*1º caso* $a\in\mathbb{N}$ e $b\notin\mathbb{N}$. Seja $b=-t$, com $t\in\mathbb{N}$. Então $ab=a(-t)=-(at)$, pelo item (iv) da Definição 9.2. Como $at$ está definido, vemos que $ab$ é o oposto deste. Exemplo: $2(-3)=-(2\cdot 3)=-6$.

*2º caso* $a,b\notin\mathbb{N}$. Sejam $a=-s$ e $b=-t$, com $s,t\in\mathbb{N}$. Então $ab=(-s)(-t)=st$, pelo item (v) da Definição 9.2. Como $st$ está definido, vemos que $ab$ é o produto de seus opostos. Exemplo: $(-2)(-3)=2\cdot 3=6$.

**Problema 9.4.2.** Use a Definição 9.2 para verificar as relações (9.3).

**Problema 9.4.3.** Demonstre o 3º caso do Problema Resolvido 9.6.

**Problema 9.4.4.** Demonstre a propriedade comutativa da multiplicação em $\mathbb{Z}$. Isto é, $ab = ba$ quaisquer que sejam $a, b \in \mathbb{Z}$.

**Problema 9.4.5.** Demonstre a propriedade associativa da multiplicação em $\mathbb{Z}$. Isto é, $(ab)c = a(bc)$ quaisquer que sejam $a, b, c \in \mathbb{Z}$.

**Problema 9.4.6.** Demonstre a propriedade distributiva da multiplicação em relação à adição em $\mathbb{Z}$. Isto é, $a(b + c) = ab + ac$ quaisquer que sejam $a, b, c \in \mathbb{Z}$.

**Problema 9.4.7.** No Teorema 4.5 vimos a Lei de Integridade, isto é, se $a$ e $b$ são números naturais tais que $ab = 0$, então $a = 0$ ou $b = 0$. Estenda a validade dessa lei para $\mathbb{Z}$.

**Problema 9.4.8. a)** Demonstre que para todo $a \in \mathbb{Z}$ se tem $a+0 = a = 0+a$. Por causa dessa propriedade 0 chama-se *elemento neutro da adição*. Prove que o elemento neutro da adição é único. Isto é, dado $a \in \mathbb{Z}$, se $b \in \mathbb{Z}$ é tal que $a + b = a$ então $b = 0$. **b)** Demonstre que para todo $a \in \mathbb{Z}$ se tem $0a = 0 = a0$. **c)** Demonstre que para todo $a \in \mathbb{Z}$ se tem $1a = a = a1$. Por causa dessa propriedade 1 chama-se *elemento neutro da multiplicação*. Prove que o elemento neutro da multiplicação é único para todo $a \neq 0$.

**Problema 9.4.9. a)** Demonstre que $a < b \Rightarrow -b < -a$ quaisquer que sejam $a, b \in \mathbb{Z}$. **b)** Demonstre a transitividade da relação de ordem. Isto é, $a < b$ e $b < c \Rightarrow a < c$ quaisquer que sejam $a, b, c \in \mathbb{Z}$.

**Problema 9.4.10.** Demonstre a Lei da Tricotomia em $\mathbb{Z}$. Isto é, quaisquer que sejam $a, b \in \mathbb{Z}$, exatamente uma das seguintes condições é verificada: $a = b$ ou $a < b$ ou $b < a$.

**Problema 9.4.11.** Demonstre as seguintes leis de compatibilidade e de cancelamento. **a)** $a < b \iff a + c < b + c$ quaisquer que sejam $a, b, c \in \mathbb{Z}$. **b)** $a = b \iff a + c = b + c$ quaisquer que sejam $a, b, c \in \mathbb{Z}$. **c)** $a < b \iff ac < bc$ quaisquer que sejam $a, b, c \in \mathbb{Z}$ com $c > 0$. **d)** $a < b \iff bc < ac$ quaisquer que sejam $a, b, c \in \mathbb{Z}$ com $c < 0$. **e)** $a = b \iff ac = bc$ quaisquer que sejam $a, b, c \in \mathbb{Z}$ com $c \neq 0$.

**Problema 9.4.12.** Explique por que valem em $\mathbb{Z}$ as fórmulas subtrativas da Seção 3.3.

*Exemplos:*

*Fórmula 3.5*: $a - c = b - c \iff a = b$, quaisquer que sejam $a, b, c \in \mathbb{Z}$. Temos:
$a - c = b - c \iff a + (-c) = b + (-c)$ (Definição 9.4) $\iff a = b$ (Problema 9.4.11 b).

*Fórmula 3.6*: $a - b = c \iff a = b + c \iff a - c = b$, quaisquer que sejam $a, b, c \in \mathbb{Z}$. Temos:
$a - b = c \iff a + (-b) = c \iff [a + (-b)] + b = b + c \iff a + [(-b) + b] = b + c \iff a + 0 = b + c \iff a = b + c$. Trocando $b$ com $c$ se obtém a outra parte. □

**Problema 9.4.13.** Quaisquer que sejam $m, n \in \mathbb{Z}$, temos: **a)** $|m| \geq 0$. **b)** $|m| = 0 \iff m = 0$. **c)** $|-m| = |m|$. **d)** $|mn| = |m||n|$. **e)** $|m \pm n| \leq |m| + |n|$. **f)** $|m| \leq n \iff -n \leq m \leq n$.

## 9.5 Princípios fundamentais

Vimos nos capítulos 1 e 4 que os números naturais $\mathbb{N} = \{0, 1, 2, 3, 4, \dots\}$ foram construídos obedecendo a alguns princípios fundamentais, que sintetizamos a seguir:

**P0** Zero é um número natural.

**P1** Todo número natural $n$ tem um sucessor, e este sucessor é único.

**P2** Todo número natural $n \neq 0$ tem um antecessor, e este antecessor é único. O número 0 não tem antecessor em $\mathbb{N}$.

**P3** Seja $S \subset \mathbb{N}$ um subconjunto com as seguintes propriedades: (i) $0 \in S$; (ii) se $n \in S$ então o sucessor de $n$ também está em $S$. Nessas condições $S = \mathbb{N}$.

Essas são as propriedades assumidas na construção psicológica dos números naturais. A propriedade P3 é mais difícil de ser percebida. Ela significa que o conjunto dos números naturais é único.

Existe uma formulação mais técnica dessas propriedades, denominadas *axiomas de Peano*, em homenagem ao matemático Giuseppe Peano, que as publicou em 1889.

Dentre os princípios acima desejamos reformular P3 da seguinte forma:

**Princípio de Indução** Seja $S \subset \mathbb{N}$ um subconjunto com as seguintes propriedades: (i) $0 \in S$; (ii) se $n \in S$ então $n + 1 \in S$. Nessas condições $S = \mathbb{N}$.

Vimos na Seção 3.4 o

**Princípio do Menor Número Natural** Se $A$ é um subconjunto não vazio do conjunto dos números naturais, então $A$ tem um menor elemento.

Isso significa que existe $a \in A$ tal que $a \leq b$ para todo $b \in A$. O Princípio de Indução e o Princípio do Menor Número Natural são equivalentes, o que é observado nos Problemas 9.6.1 e 9.6.2.

Vamos estender o Princípio do Menor Número Natural para subconjuntos de $\mathbb{Z}$. Começamos com algumas definições. Dado um subconjunto não vazio $A$ de $\mathbb{Z}$, dizemos que $A$ é *limitado inferiormente* se existe $m \in \mathbb{Z}$ tal que $m \leq a$ para todo $a \in A$. Nesse caso chamamos $m$ de *limitante inferior*. Por outro lado, $A$ se diz *limitado superiormente* se existe $M \in \mathbb{Z}$ tal que $a \leq M$ para todo $a \in A$. Nesse caso chamamos $M$ de *limitante superior*. Dizemos que $A$ tem *máximo* se existir $M \in A$ tal que $a \leq M$ para todo $a \in A$. Dizemos que $A$ tem *mínimo* se existir $m \in A$ tal que $m \leq a$ para todo $a \in A$.

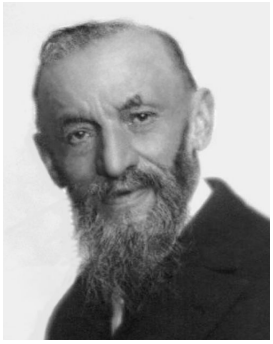


Figura 9.1. Giuseppe Peano, matemático italiano e professor da Universidade de Turim, foi um dos fundadores da Lógica Matemática e da Teoria dos Conjuntos. Contribuiu particularmente para a compreensão moderna do Método da Indução Completa, que estudamos, neste texto, no Capítulo 10. Contribuiu também com a Análise, Equações Diferenciais, Análise Vetorial, assim como com o ensino do Cálculo Diferencial e Integral. Ao lado, foto de Giuseppe Peano (mais detalhes na página 262).

**Teorema 9.7.** *Todo subconjunto não vazio de $\mathbb{Z}$ limitado inferiormente tem mínimo. Todo subconjunto não vazio de $\mathbb{Z}$ limitado superiormente tem máximo.*

*Demonstração.* Seja $A \subset \mathbb{Z}$ com $A \neq \emptyset$ e limitado inferiormente. Seja $m$ um limitante inferior de $A$. Consideremos o conjunto $A - m = \{a - m \mid a \in A\}$. Vemos que $A - m \subset \mathbb{N}$ e $A - m \neq \emptyset$, portanto, em virtude do Princípio do Menor Número Natural, $A - m$ tem mínimo, digamos, $l$. Como $l \in A - m$, existe $m_0 \in A$ tal que $l = m_0 - m$. Então, para todo $a \in A$, temos $l \leq a - m \Rightarrow m_0 - m \leq a - m \Rightarrow m_0 \leq a$. Portanto, $m_0$ é mínimo de $A$.

Por outro lado, seja $A \subset \mathbb{Z}$ com $A \neq \emptyset$ e limitado superiormente. Consideremos o conjunto $-A = \{-a \mid a \in A\}$. Vemos que $-A$ é limitado inferiormente, portanto tem mínimo. O oposto desse mínimo é máximo de $A$. □

## 9.6 Problemas

**Problema 9.6.1.** Demonstre que o Princípio do Menor Número Natural implica no Princípio de Indução.

**Problema 9.6.2.** Estude a seguinte demonstração de que o Princípio de Indução implica no Princípio do Menor Número Natural. Seja $S$ um subconjunto não vazio de $\mathbb{N}$. Seja $M$ o conjunto dos números naturais $m$ tais que $m \leq s$ para todo $s$ em $S$. Temos $0 \in M$. Ainda, se $s \in S$ então $s+1 \notin M$. Portanto $M \neq \mathbb{N}$ e pelo princípio da indução existe um número natural $l$ tal que $l + 1 \notin M$. Afirmamos que $l$ é o mínimo de $S$. De fato, como $l \in M$ então $l \leq s$ para todo $s \in S$, por definição de $M$. Ainda, se $l \notin S$ então $l < s$ para todo $s \in S$, e $l + 1 \leq s$ para todo $s \in S$, contradizendo que $l + 1 \notin M$. Segue que $l \in S$, que é assim o mínimo de $S$.

## 9.7 Teoria dos números inteiros

Nesta seção estendemos para o conjunto $\mathbb{Z}$ os conceitos da Teoria dos Números Naturais estudados nos capítulos 4 e 5. Adaptamos o algoritmo da divisão e as definições e resultados sobre divisibilidade, mdc, mmc e números primos e compostos. Sobre classes módulo $m$, consulte a Seção 9.11.

**Teorema 9.8** (Algoritmo da Divisão)**.** *Dados números inteiros $a$ e $b \neq 0$, existe e é único o par de números inteiros $q$ e $r$ tal que*

$$a = bq + r, \quad \text{com } 0 \leq r < |b|.$$

*Demonstração.* Primeiro estabelecemos a existência de $q$ e $r$. Suponhamos inicialmente $b > 0$. Notemos que o conjunto

$$A = \{a - nb \mid n \in \mathbb{Z} \text{ e } a - nb \geq 0\}$$

é não vazio. De fato, tomando $n = -|a|$ temos $a - nb = a + |a|b \geq a + |a| \geq 0$ pois $b \geq 1$. Como $A \subseteq \mathbb{N}$, aplicando o Princípio do Menor Número Natural, vemos que $A$ tem mínimo. Seja $r$ esse mínimo. Como $r \in A$ temos $r \geq 0$ e existe $q \in \mathbb{Z}$ tal que $r = a - qb$, ou $a = qb + r$. Por outro lado, como $a - (q+1)b < a - qb$ e $a - qb = r$ é o mínimo de $A$, então $a - (q+1)b < 0 \Rightarrow r < b \Rightarrow r < |b|$.

Supomos agora $b < 0$. Então $-b > 0$, e o resultado acima diz que existem inteiros $q'$ e $r$ tais que $a = (-b)q' + r$, com $0 \leq r < -b$. Como $-b = |b|$ temos $0 \leq r < |b|$. Pondo $q = -q'$ temos $a = bq + r$. Isso estabelece a existência de $q$ e $r$.

Vejamos a unicidade. Sejam $q$ e $r$ números inteiros tais que $a = bq + r$ e $0 \leq r < |b|$, e sejam $p$ e $s$ números inteiros tais que $a = bp + s$ e $0 \leq s < |b|$. Subtraindo membro a membro essas identidades vem $s - r = b(q - p) \Rightarrow |s - r| = |b||q - p|$. Como $0 \leq r < |b|$ e $0 \leq s < |b|$ temos $|s - r| < |b| \Rightarrow |b||q - p| < |b| \Rightarrow 0 \leq |q - p| < 1 \Rightarrow |q - p| = 0$. Segue que $q = p$. De $s - r = b(q - p)$ obtemos $s - r = 0 \Rightarrow s = r$. Fica demonstrada a unicidade do par $q$ e $r$. □

Dados números inteiros $a$ e $b \neq 0$, os números inteiros $q$ e $r$ tais que $a = bq + r$ e $0 \leq r < |b|$ são denominados, respectivamente, *quociente* e *resto* da divisão euclidiana de $a$ por $b$.

Agora adaptamos a Definição 4.18:

**Definição 9.9.** Um número inteiro $a$ se diz *múltiplo* de um número inteiro $b$ se existir um número inteiro $q$ tal que $a = bq$. Nesse caso, e se $b \neq 0$, dizemos também que $b$ *divide* $a$, ou que $b$ é *divisor* ou *fator* de $a$.

Se $a$ e $b \neq 0$ são inteiros tais que $a = bq$ para algum número inteiro $q$, anotamos $b \mid a$. Por outro lado, se não existir tal inteiro $q$, anotamos $b \nmid a$. Observe que, de acordo com o Teorema do Algoritmo da Divisão, existem inteiros $q$ e $r$ tais que $a = bq + r$ e $0 \leq r < |b|$. Dessa forma, se $r = 0$ temos $b \mid a$, e se $r > 0$, temos $b \nmid a$.

Apresentamos a seguir uma coletânea de propriedades derivadas do conceito de divisibilidade. O estudante certamente já trabalhou com a maioria delas. No que segue $a$, $b$, $c$, $d$, $m$ e $n$ são inteiros quaisquer. Sempre que se escrever $a \mid b$ se entende que $a \neq 0$.

**1.** $a \mid 0$, $1 \mid a$, $a \mid a$;

**2.** $a \mid b \iff -a \mid b \iff a \mid -b \iff -a \mid -b$;

**3.** $a \mid 1 \iff a = \pm 1$;

**4.** $a \mid b$ e $a \mid c \Rightarrow a \mid mb + nc$;

**5.** $a \mid b$ e $b \mid c \Rightarrow a \mid c$;

**6.** $a \mid b$ e $c \mid d \Rightarrow ac \mid bd$;

**7.** $a \mid b$ e $b \mid a \iff a = \pm b$;

**8.** $a \mid b$ e $b \neq 0 \Rightarrow |a| \leq |b|$.

A Propriedade 2 pode ser reescrita da seguinte forma: $a \mid b \iff |a| \mid |b|$. A Propriedade 4, por sua vez, se generaliza da seguinte forma: se $b_i$ e $n_i$ são inteiros para $1 \leq i \leq t$ e se $a \mid b_i$ para todo $i$, então $a \mid (n_1 b_1 + \cdots + n_t b_t)$.

A seguir adaptamos para $\mathbb{Z}$ a definição de mdc já estudada em 5.10. Dado um número inteiro $a$, indicamos (também) por $\mathcal{D}(a)$ o conjunto dos números inteiros divisores de $a$. Observamos que 1 está em $\mathcal{D}(a)$ qualquer que seja $a \in \mathbb{Z}$, e que se $a \neq 0$ então $\mathcal{D}(a)$ é finito. Portanto, dados números inteiros $a$ e $b$ não simultaneamente nulos, o conjunto $\mathcal{D}(a) \cap \mathcal{D}(b)$ é não vazio e finito. Segue que $\mathcal{D}(a) \cap \mathcal{D}(b)$ tem um elemento máximo. Isso justifica a seguinte definição.

**Definição 9.10.** Dados números inteiros $a$ e $b$ não simultaneamente nulos, o elemento máximo do conjunto $\mathcal{D}(a) \cap \mathcal{D}(b)$ chama-se *máximo divisor comum* de $a$ e $b$, e é indicado por $\text{mdc}(a, b)$. Se $a = 0$ e $b = 0$ convém definir $\text{mdc}(0, 0) = 0$.

As mesmas observações se aplicam para três ou mais números inteiros $a_1$, $a_2$, ..., $a_n$, e da mesma forma se define $\text{mdc}(a_1, a_2, \ldots, a_n)$.

Das considerações acima podemos ver que, dados inteiros $a$ e $b$, o valor de $\mathrm{mdc}(a,b)$ depende apenas dos divisores positivos de $a$ e $b$. Portanto $\mathrm{mdc}(a,b) = \mathrm{mdc}(|a|,|b|)$. Dessa forma, as propriedades do mdc vistas nas seções 5.10 e 7.2 se estendem naturalmente de $\mathbb{N}$ para $\mathbb{Z}$, com as devidas adaptações. Por exemplo, a identidade $\mathrm{mdc}(ta,tb) = t\,\mathrm{mdc}(a,b)$ do Teorema 7.2 tem em $\mathbb{Z}$ a forma $\mathrm{mdc}(ta,tb) = |t|\,\mathrm{mdc}(a,b)$ quaisquer que sejam os inteiros $a$, $b$ e $t$.

O mesmo ocorre com o mmc. Dados inteiros $a$ e $b$, definimos $\mathrm{mmc}(a,b)$ como o menor dentre os múltiplos comuns positivos de $a$ e $b$. Portanto $\mathrm{mmc}(a,b) = \mathrm{mmc}(|a|,|b|)$.

Existe, entretanto, uma propriedade adicional do mdc que necessitamos estudar, pois a utilizamos no Capítulo 11. Começamos com um exemplo, considerando $a = 1365$ e $b = 231$. No Problema Resolvido 5.18, vimos que $\mathrm{mdc}(1365, 231) = 21$. Estamos interessados em saber o que são as combinações lineares $1365m + 231n$, com $m, n \in \mathbb{Z}$. Fazendo cálculos, escolhemos algumas combinações com valores baixos: $1\cdot 1365 + (-5)\cdot 231 = 210$, $1\cdot 1365 + (-6)\cdot 231 = -21$, $2\cdot 1365 + (-11)\cdot 231 = 189$, $2\cdot 1365 + (-12)\cdot 231 = -42$, $2\cdot 1365 + (-10)\cdot 231 = 420$. Em outros termos

$$M = \{1365m + 231n \mid m, n \in \mathbb{Z}\} = \{\ldots, -42, -21, 189, 210, 420, \ldots\},$$

que sugere ser $M$ um conjunto de múltiplos de $\mathrm{mdc}(1365, 231) = 21$. Em verdade temos o

**Teorema 9.11.** *Se $a, b \in \mathbb{Z}$, então o conjunto das combinações lineares de $a$ e $b$, definido por*

$$M = \{am + bn \mid m, n \in \mathbb{Z}\},$$

*coincide com o conjunto dos múltiplos de* $\mathrm{mdc}(a,b)$.

*Demonstração.* Notemos inicialmente que se $a = 0$ e $b = 0$ então $M = \{0\}$ e $\mathrm{mdc}(0,0) = 0$, portanto o resultado vale nesse caso. Suponhamos $a \neq 0$ ou $b \neq 0$. Consideremos o conjunto

$$M_+ = \{am + bn \mid m, n \in \mathbb{Z} \text{ e } am + bn > 0\}.$$

Vejamos que $M_+ \neq \emptyset$. Se $a \neq 0$ então $a\cdot 1 + b\cdot 0 \in M_+$ ou $-a\cdot 1 + b\cdot 0 \in M_+$. Se $a = 0$ então $b \neq 0$, e $b \in M_+$ ou $-b \in M_+$. Assim $M_+$ é não vazio. Como $M_+ \subset \mathbb{N}$, aplicando o Princípio do Menor Número Natural, consideramos o mínimo $d$ de $M_+$. Provemos que $d = \mathrm{mdc}(a,b)$.

Notemos primeiro que $d > 0$ e que existem inteiros $m_0$ e $n_0$ tais que $d = am_0 + bn_0$, já que $d \in M_+$. Portanto, se $t$ é um divisor comum de $a$ e $b$ então $t \mid am_0 + bn_0 \Rightarrow t \mid d$, o que implica $t \leq d$. Por outro lado, se $a = qd + r$, com $q$ e $r$ inteiros tais que $0 \leq r < d$, temos $r = 0$. De fato, $r = a - qd = a - q(am_0 + bn_0) = a(1 - qm_0) + b(-qn_0)$. Logo $r$ é uma combinação linear de $a$ e $b$. Mas $0 \leq r < d$. Como $d$ é o mínimo de $M_+$ temos que ter $r \notin M_+ \Rightarrow r = 0$. Disso segue que $d \mid a$. Da mesma forma se demonstra que $d \mid b$.

Em resumo, $d$ é um divisor comum de $a$ e $b$ e é maior do que ou igual a qualquer outro divisor comum. Concluímos que $d = \mathrm{mdc}(a,b)$.

Para terminar a demonstração do Teorema e provar que $M$ coincide com o conjunto dos múltiplos de $d$, basta observar o seguinte. Todo $am + bn \in M$ é múltiplo de $d$, pois $d \mid a$ e $d \mid b$ $\Rightarrow d \mid am + bn$. Por outro lado, se $t$ é múltiplo de $d$, escrevemos $t = qd$ para algum inteiro $q$, e $t = q(am_0 + bn_0) = a(qm_0) + b(qn_0) \in M$. □

Do que foi estudado acima destacamos o seguinte resultado:

**Escólio 9.12.** *Dados $a, b \in \mathbb{Z}$ existem inteiros $m$ e $n$ tais que* $\mathrm{mdc}(a,b) = am + bn$.

Observamos que nas combinações $am+bn$ existe uma infinidade de repetições. Por exemplo, $21 = 10 \cdot 1365 - 59 \cdot 231 = 21 \cdot 1365 - 124 \cdot 231 = 32 \cdot 1365 - 189 \cdot 231$ etc. Veremos logo abaixo como usar o algoritmo euclidiano para calcular $m$ e $n$ tais que $am + bn = \text{mdc}(a, b)$.

A definição de inteiros relativamente primos é análoga à de naturais relativamente primos.

**Definição 9.13.** Os números inteiros $a$ e $b$ chamam-se *relativamente primos* se $\text{mdc}(a, b) = 1$. Nesse caso $a$ e $b$ também são denominados *primos entre si* ou *coprimos*. Da mesma forma, se os números inteiros $a_1$, $a_2$, ..., $a_n$ são tais que $\text{mdc}(a_1, a_2, \ldots, a_n) = 1$, dizemos que são relativamente primos (ou primos entre si, ou ainda coprimos).

Uma consequência imediata do Escólio 9.12 é

**Corolário 9.14.** *Sejam $a$ e $b$ inteiros. Então $a$ e $b$ são relativamente primos se, e somente se, existem inteiros $m$ e $n$ tais que $am + bn = 1$.*

*Demonstração.* Se $a$ e $b$ são relativamente primos temos $\text{mdc}(a, b) = 1$, e vimos que existem inteiros $m$ e $n$ tais que $am + bn = 1$. Por outro lado, se existem inteiros $m$ e $n$ tais que $am + bn = 1$ e se $d = \text{mdc}(a, b)$, como $d \mid a$ e $d \mid b$ temos $d \mid am + bn = 1$, em consequência $d = 1$. Portanto $a$ e $b$ são relativamente primos. □

**Problema resolvido 9.15.** Calcule inteiros $m$ e $n$ tais que $\text{mdc}(-1071, 85) = m(-1071)+n85$.

*Solução.* Para calcular $\text{mdc}(-1071, 85)$ podemos considerar $\text{mdc}(1071, 85)$, pois os dois valores são iguais. Efetuamos as divisões sucessivas:

$$\begin{aligned} 1071 &= 12 \cdot 85 + 51 \\ 85 &= 1 \cdot 51 + 34 \\ 51 &= 1 \cdot 34 + 17 \\ 34 &= 2 \cdot 17 + 0 \end{aligned}$$

Vemos que o último resto não nulo é 17, portanto $\text{mdc}(-1071, 85) = 17$. Para obter os inteiros $m$ e $n$ usamos as relações acima, iniciando com a penúltima:
$17 = 51 - 1 \cdot 34 = 51 - 1(85 - 1 \cdot 51) = 51 - 1 \cdot 85 + 51 = 2 \cdot 51 - 1 \cdot 85 = 2(1071 - 12 \cdot 85) - 1 \cdot 85 = 2 \cdot 1071 - 24 \cdot 85 - 1 \cdot 85 = 2 \cdot 1071 - 25 \cdot 85$. Portanto $\text{mdc}(-1071, 85) = (-2)(-1071) + (-25)85$. Portanto podemos tomar $m = -2$ e $n = -25$. □

**Problema resolvido 9.16.** Para todo $k \in \mathbb{Z}$, calcule $\text{mdc}(4k + 3, 5k + 4)$.

*Solução.* O estudante pode verificar que em $\mathbb{Z}$ vale o resultado: "Se $a$, $b$, $q$ e $r$ são números inteiros tais que $a = bq + r$, então $\text{mdc}(a, b) = \text{mdc}(b, r)$". No contexto dos números naturais isso corresponde ao Teorema 5.15.

Como $5k + 4 = 1 \cdot (4k + 3) + (k + 1)$ e $4k + 3 = 3 \cdot (k + 1) + k$ e $k + 1 = 1 \cdot k + 1$ vem $\text{mdc}(5k + 4, 4k + 3) = \text{mdc}(4k + 3, k + 1) = \text{mdc}(k + 1, k) = \text{mdc}(1, k) = 1$ para todo $k \in \mathbb{Z}$. □

As definições de inteiro primo ou composto assim como suas propriedades se adaptam com poucas modificações em relação ao que já conhecemos dos números naturais.

**Definição 9.17.** Denominamos *primo* a todo número inteiro $> 1$ que não tem divisor positivo diferente de 1 e dele mesmo. Chamamos de *composto* a todo número inteiro $a \neq 0$ que tem divisor positivo diferente de 1 e de $|a|$.

Portanto, os primos são os mesmos de $\mathbb{N}$. As propriedades dos primos estudadas anteriormente, particularmente as do Capítulo 7, se estendem para $\mathbb{Z}$ com as devidas adaptações. Por exemplo, o Corolário 7.4 passa a ter a seguinte redação: "Se $p$ é primo e se $p$ é divisor de $ab$ então $p$ é divisor de $a$ ou de $b$, quaisquer que sejam os números inteiros $a$ e $b$". Também vale que todo inteiro $n$ diferente de $-1$, 0 ou 1 tem uma única decomposição como produto de primos, a menos da ordem dos fatores. Para isso basta tomar para $n < -1$ o oposto da decomposição em primos de $|n|$. Por exemplo, $-12 = -2^2 \cdot 3$.

Quanto aos compostos, $a \in \mathbb{Z}$ é composto se, e somente se, $|a|$ é composto. Portanto, os inteiros compostos são os compostos de $\mathbb{N}$ e seus opostos. Em particular, compostos em $\mathbb{Z}$ são $\neq$'s de $-1$, 0, e 1.

No Problema 7.10.7 vimos que se $p$ é primo então $p$ é divisor de $2^p - 2$. Será útil para nós a seguinte generalização, denominada Pequeno Teorema de Fermat:

**Teorema 9.18.** *Se $p$ é primo, então ele é divisor de $a^p - a$ para todo inteiro $a$.*

Uma consequência: como $a^p - a = a(a^{p-1} - 1)$, se $p \nmid a$, então $p \mid a^{p-1} - 1$. A demonstração mais simples desse teorema usa o Método da Indução Completa, e a veremos no próximo capítulo.

## 9.8 Problemas

**Problema 9.8.1.** Demonstre a última afirmação desta seção: $a \in \mathbb{Z}$ é composto se, e somente se, $|a|$ é composto. Explique por que os compostos em $\mathbb{Z}$ são $\leq -4$ ou $\geq 4$.

**Problema 9.8.2.** Alguns autores definem como primos inteiros tanto os primos naturais como seus opostos. Imagine as razões pelas quais não fizemos isso aqui.

**Problema 9.8.3.** Explique por que a relação do Escólio 7.18 se escreve, em $\mathbb{Z}$, como $\text{mmc}(a, b)\,\text{mdc}(a, b) = |ab|$.

**Problema 9.8.4.** Calcule inteiros $m$ e $n$ tais que $\text{mdc}(17290, -3553) = n17290 + m(-3553)$.

**Problema 9.8.5.** Encontre condições necessárias e suficientes sobre os inteiros $a$ e $b$ para que $\text{mdc}(a, b) = |a|$.

**Problema 9.8.6.** Para todo $k \in \mathbb{Z}$, calcule: **a)** $\text{mdc}(2k + 1, 9k + 4)$; **b)** $\text{mdc}(2k - 1, 9k + 4)$.

**Problema 9.8.7.** Determinar todos os inteiros positivos $x$ e $y$ tais que $\text{mdc}(x, y) = 18$ e $\text{mmc}(x, y) = 72$.

**Problema 9.8.8.** Demonstre que se $a$, $b$ e $c$ são inteiros ímpares, então a equação $ax^2+bx+c = 0$ não tem raiz racional.

**Problema 9.8.9.** Determine o menor inteiro positivo $m$ tal que $10125m$ é simultaneamente um quadrado perfeito e um número cúbico.

**Problema 9.8.10.** Sejam $a$ e $b$ inteiros não simultaneamente nulos e seja $d = \text{mdc}(a, b)$. Se $r$ e $s$ são inteiros tais que $ar + bs = d$, o que pode ser $\text{mdc}(r, s)$?

## 9.9 Problemas adicionais

**Problema 9.9.1.** [Potências com base negativa] Estenda a definição de potência $a^n$ para bases negativas inteiras. Verifique se valem as fórmulas usuais $a^{m+n} = a^m a^n$, $(a^m)^n = a^{mn}$ e $a^m b^m = (ab)^m$, para $a$ e $b$ inteiros não nulos e $m, n \geq 0$.

**Problema 9.9.2.** **a)** Veja quais fórmulas envolvendo o mdc e o mmc podem ser generalizadas para três números inteiros ou mais. **b)** Em particular, mostre que, dados inteiros $a_1$, $a_2$, ..., $a_n$, existem inteiros $x_1$, $x_2$, ..., $x_n$ tais que $x_1a_1 + x_2a_2 + \cdots + x_na_n = \text{mdc}(a_1, \ldots, a_n)$. **c)** Encontre inteiros $\ell$, $m$ e $n$ tais que $561\ell + 429m + 63n = \text{mdc}(561,\ 429,\ 63)$.

**Problema 9.9.3.** Sejam $a$, $b$ e $c$ inteiros tais que $a \mid b$. Se $\text{mdc}(b, c) = 1$, então $\text{mdc}(a, c) = 1$.

**Problema 9.9.4.** Sejam $a$ e $b$ inteiros. Se $\text{mdc}(a, b) = 8$, quais são os possíveis valores de $\text{mdc}(a^3, b^4)$?

**Problema 9.9.5.** Sejam $a$ e $b$ inteiros e $p$ primo. Se $\text{mdc}(a, b) = p^3$, calcule $\text{mdc}(a^2, b^2)$.

**Problema 9.9.6.** Se $a$ e $b$ são inteiros tais que $17 \mid 2a + 3b$, então $17 \mid 9a + 5b$.

**Problema 9.9.7.** Prove que dentre dez inteiros consecutivos quaisquer pelo menos um deles é relativamente primo com cada um dos outros.

## 9.10 Temas para investigação

**Tema 9.10.1.** No Problema 3.9.13 vimos que para todo número natural $n$ os dígitos das unidades das representações decimais de $n$ e $n^5$ são iguais. Vamos aprofundar esse resultado. Justifique por que os dígitos das unidades das representações decimais dos números naturais $a$ e $b$ são iguais se e somente se $10|a - b$. Demonstre que $10 \mid n^5 - n$ para todo número natural $n$, agora usando o Pequeno Teorema de Fermat 9.18. Da mesma forma prove que $10 \mid n^9 - n$. Encontre todos os números naturais $k$ tais que para todo $n$ os dígitos das unidades das representações decimais de $n$ e $n^k$ são iguais.

**Tema 9.10.2.** Dado um primo $p$, investigue para quais números naturais $q$ é verdadeira a seguinte afirmação:

$$p \text{ divide } a^q - a \quad \text{ para todo } a \in \mathbb{N}.$$

**Tema 9.10.3.** Vimos no Tema 5.16.8 o que são os números de Mersenne $M_p = 2^p - 1$, com $p$ primo. Vimos também que existe, desde o tempo dos antigos gregos, um interesse em determinar para quais primos $p$ se tem $M_p$ primo, pois esses primos entram na composição dos números perfeitos pares (confira página 178).

Para obter informações sobre a natureza dos números $M_p = 2^p - 1$ podemos proceder indutivamente, e examinar a forma desses números para uma certa quantidade de valores de $p$. Se pudermos obter conjecturas que nos pareçam razoáveis, podemos em seguida estudar como demonstrá-las (ou eventualmente construir contra-exemplos). Confira a tabela abaixo.

**a)** Examinando a tabela tente observar um padrão de comportamento entre os números de Mersenne e os primos que fazem parte de sua decomposição canônica. Faça uma conjectura geral. Em outros termos, se $q$ é um fator primo de $M_p = 2^p - 1$, qual é sua forma presumível?

**b)** Usando esse critério encontre um fator primo de $2^{37}-1$ (ou conjecture que esse número é primo).
**c)** Investigue uma demonstração de sua conjectura.
**d)** Investigue como são os fatores primos de $2^n-1$ quando $n$ não é primo. Faça suas conjecturas. Alguma demonstração?

| $p$ | valor de $2^p-1$ | decomposição em primos |
|---|---|---|
| 2 | 3 | 3 (primo) |
| 3 | 7 | 7 (primo) |
| 5 | 31 | 31 (primo) |
| 7 | 127 | 127 (primo) |
| 11 | 2047 | $23 \cdot 89$ |
| 13 | 8191 | 8191 (primo) |
| 17 | 131 071 | 131 071 (primo) |
| 19 | 524 287 | 524 287 (primo) |
| 23 | 8 388 607 | $47 \cdot 178\,481$ |
| 29 | 536 870 911 | $233 \cdot 1103 \cdot 2089$ |
| 31 | 2 147 483 647 | 2 147 483 647 (primo) |

**Tema 9.10.4. a)** Vimos no Tema 9.10.3 acima conjecturas e resultados sobre os fatores primos de $2^n-1$. Faça o mesmo para $3^n-1$. Obtenha uma possível forma geral dos divisores primos de $3^p-1$, para $p$ primo. Veja se é possível usar isso para encontrar um divisor primo ímpar de $3^{31}-1$. E quanto aos divisores primos de $3^n-1$ para $n$ composto? Alguma conjectura? Alguma demonstração? **b)** Alguma generalização para $a^n-1$?

**Tema 9.10.5.** Vimos no Problema 6.6.4 que se 3 divide $a^2+b^2$ então 3 divide $a$ e $b$, quaisquer que sejam os números naturais $a$ e $b$. Investigue quais são os números primos $p$ para os quais vale a seguinte implicação: "se $p$ é primo e se $p$ divide $a^2+b^2$, sendo $a$ e $b$ números naturais, então $p$ divide $a$ e $b$". Alguma conjectura? Alguma demonstração? O que ocorre quando $p$ não é primo?

**Tema 9.10.6.** Investigue o que podem ser: **i)** $\text{mdc}(a^{2^m}+1, a^{2^n}+1)$ com $a$, $m$ e $n$ números naturais (quais condições convém colocar sobre esses números?); **ii)** $\text{mdc}(2^a-1, 2^b-1)$ com $a$ e $b$ números naturais.

**Tema 9.10.7.** Dado um inteiro positivo $n \geq 2$, defina $f(n)$ como o maior inteiro $k$ tal que

$$k \mid x^n - x \quad \text{para todo } x \in \mathbb{Z}$$

Investigue o problema de encontrar $f(n)$. Em particular, verfique que $f(2)=2$, $f(3)=6$, $f(4)=2$ e $f(5)=30$.

## 9.11 Protocolo de Gauss para as congruências

Temos visto fartamente neste texto a importância do algoritmo da divisão para nossos estudos e investigações em Teoria dos Números. Vimos, em particular, como esse algoritmo gera as denominadas classes módulo $r$ (o resto da divisão euclidiana). Até agora usamos uma metodologia, digamos assim, mais "pé no chão".

O genial matemático Johann C. F. Gauss introduziu, em seu livro *Disquisitiones Arithmeticae*, de 1801, uma notação muito funcional para as congrências. Vejamos, em resumo, do que se trata e como usá-la em algumas situações mais simples.

**Definição 9.19.** Seja $m > 1$ um número inteiro. Os inteiros $a$ e $b$ se dizem *congruentes módulo* $m$ quando $m \mid a - b$. Nesse caso anotamos $a \equiv b \pmod{m}$.

**Exemplo 9.20.** $23 \equiv 13 \pmod{5}$, pois $5 \mid 23 - 13$.

Façamos observações iniciais. Se $m \mid a - b$, existe $q$ tal que $a - b = qm$, ou $a = qm + b$. Portanto $b$ é um resto da divisão de $a$ por $m$, mas não necessariamente é o resto da divisão euclidiana. No exemplo dado, temos $23 \equiv 18 \equiv 13 \equiv 8 \equiv 3 \pmod{5}$, e apenas 3 é o resto da divisão euclidiana de 23 por 5.

Na observação acima introduzimos ao estudante uma das maravilhas da notação de Gauss: podemos concatenar as congruências. Significa que $23 \equiv 18 \pmod{5}$, $23 \equiv 13 \pmod{5}$, $18 \equiv 13 \pmod{5}$, etc. o estudante pode conferir.

Se $r$ é o resto da divisão euclidiana de $a$ por $m$, então $a = qm + r$, $0 \leq r < m$. Portanto $qm = a - r$, e $a \equiv r \pmod{m}$. Nesse caso $r$ se chama *resíduo módulo* $m$. O conjunto completo de resíduos módulo $m$ é então $\{0, 1, \ldots, m - 1\}$.

Se $a \equiv b \pmod{m}$, temos também $b \equiv a \pmod{m}$, pois, se $m \mid a - b$, com $a - b = qm$, temos $m \mid b - a$, com $b - a = (-q)m$ (lembrando que estamos no conjunto dos inteiros). Em particular, no exemplo $23 \equiv 13 \pmod{5}$ acima, temos também $13 \equiv 23 \pmod{5}$. Também vale que $-23 \equiv -13 \pmod{5}$.

Nos exemplos acima vimos que $23 \equiv 3 \pmod{5}$ e $18 \equiv 3 \pmod{5}$, portanto $23 \equiv 18 \pmod{5}$ implica que 23 e 18 têm restos iguais quando divididos por 5. É importante o seguinte resultado:

**Proposição 9.21.** *$a \equiv b \pmod{m}$ se, e somente se, $a$ e $b$ têm restos iguais quando divididos por $m$.*

*Demonstração.* Vamos começar com a recíproca: supomos que $a$ e $b$ têm restos iguais quando divididos por $m$. Logo $a = qm + r$ e $b = tm + r$. Portanto $a - qm = b - tm \Rightarrow a - b = (q - t)m$ e $m \mid a - b$. Em consequência $a \equiv b \pmod{m}$.

Supomos agora que $a \equiv b \pmod{m}$. Seja $r$ um resto da divisão de $a$ por $m$, portanto $a = qm + r$ para algum $q$. Vamos provar que $r$ também é um resto para $b$. Como $m \mid a - b$, existe $t$ tal que $a - b = tm$. Logo $qm + r - b = tm \Rightarrow b = (q - t)m + r$, e $r$ é também um resto da divisão de $b$ por $m$. □

**Corolário 9.22.** *Se $a \equiv b \pmod{m}$ e se $r$ é um resíduo de $a$ módulo $m$, então $r$ é também um resíduo de $b$ módulo $m$.*

*Demonstração.* A condição $0 \leq r < m$ não depende de $a$ ou $b$, logo basta aplicar o Teorema. □

Seguem as propriedades mais imediatas das congruências:

**Proposição 9.23.** *Seja $m > 1$ um inteiro. Quaisquer que sejam os inteiros $a$, $b$, $c$, $d$ e $k$, temos:*
*i)* $a \equiv a \pmod{m}$;
*ii) Se* $a \equiv b \pmod{m}$, *então* $b \equiv a \pmod{m}$;
*iii) Se* $a \equiv b \pmod{m}$ *e* $b \equiv c \pmod{m}$, *então* $a \equiv c \pmod{m}$;
*iv)* $a \equiv 0 \pmod{m}$ *se, e somente se, $m$ é divisor de $a$;*
*v) Se* $a \equiv b \pmod{m}$, *então* $ak \equiv bk \pmod{m}$;
*vi) Se* $a \equiv b \pmod{m}$ *e* $c \equiv d \pmod{m}$, *então* $a + c \equiv b + d \pmod{m}$;
*vii) Se* $a \equiv b \pmod{m}$ *e* $c \equiv d \pmod{m}$, *então* $ac \equiv bd \pmod{m}$;
*viii) Se* $a \equiv b \pmod{m}$, *então* $a^n \equiv b^n \pmod{m}$, *para todo inteiro* $n \geq 1$.

Temos ainda:

**Proposição 9.24.** *Sejam $m, n > 1$ inteiros. Quaisquer que sejam os inteiros $a$, $b$ e $c$, temos:*
*i)* $a \equiv b \pmod{m}$ *e* $a \equiv b \pmod{n}$ *se, e somente se,* $a \equiv b \pmod{\operatorname{mmc}(m,n)}$;
*ii) Se* $\operatorname{mdc}(m,n) = 1$, *então* $a \equiv b \pmod{m}$ *e* $a \equiv b \pmod{n}$ *se, e somente se,* $a \equiv b \pmod{mn}$.

Para não prolongar muito este apêndice, deixamos para o estudante as demonstrações. Passamos aos exemplos:

**Exemplo 9.25.** Mostre que $13 \mid 27^{421} - 1$. Como $27 \equiv 1 \pmod{13}$, temos $27^{421} \equiv 1^{421} \equiv 1 \pmod{13}$. Logo vale a afirmação.

**Exemplo 9.26.** Calcule o resto da divisão euclidiana de $2^{50\,000}$ por 17 usando congruências. Temos $2^{50\,000} \equiv (2^4)^{12500} = 16^{12500} \equiv (-1)^{12500} = 1 \pmod{17}$. Portanto, o resto é 1.

**Exemplo 9.27.** Demonstre que $7 \mid 11 \cdot 2^{6n+3} + 3 \cdot 5^{6m}$, quaisquer que sejam $m, n \geq 1$. Temos $2^{6n+3} = 8^{2n+1} \equiv 1^{2n+1} = 1 \pmod{7}$. Logo $11 \cdot 2^{6n+3} \equiv 11 \equiv 4 \pmod{7}$. Ainda $5^{6m} \equiv (-2)^{6m} = 2^{6m} = 8^{2m} \equiv 1^{2m} = 1 \pmod{7}$. Logo $3 \cdot 5^{6m} \equiv 3 \cdot 1 = 3 \pmod{7}$. Combinando os dois resultados temos $11 \cdot 2^{6n+3} + 3 \cdot 5^{6m} \equiv 4 + 3 \equiv 0 \pmod{7}$. Terminamos.

Na Seção 4.7 estudamos o conceito de classes módulo $n$. Podemos agora formalizar.

**Definição 9.28.** Seja $m > 1$ um número inteiro. Para cada inteiro $r$ tal que $0 \leq r < m$, definimos o conjunto

$$A(m, r) = \{qm + r \mid q \in \mathbb{Z}\},$$

denominado *classe módulo $m$ determinada por $r$*.

Por exemplo, se $m = 2$, temos duas classes módulo 2, que são

$$A(2, 0) = \{2q \mid q \in \mathbb{Z}\} = \{\cdots - 6, -4, -2, 0, 2, 4, 6, \ldots\}$$

e

$$A(2, 1) = \{2q + 1 \mid q \in \mathbb{Z}\} = \{\cdots - 5, -3, -1, 1, 3, 5, 7, \ldots\}$$

denominadas, respectivamente, classe dos números pares e classe dos números ímpares.

Notemos que $a \in A(m, r) \iff$ existe $q$ tal que $a = qm + r \iff m \mid a - r \iff a \equiv r \pmod{m}$. Em outros termos, $A(m, r) = \{a \in \mathbb{Z} \mid a \equiv r \pmod{m}\}$.

**Proposição 9.29.** *Seja $m > 1$ um número inteiro. Valem as seguintes propriedades:* ***a)*** *Existem $m$ classes módulo $m$.* ***b)*** *Se $r \neq s$ são inteiros tais que $0 \leq r, s < m$, então as classes $A(m, r)$ e $A(m, s)$ são disjuntas.* ***c)*** *$\mathbb{Z}$ é a reunião das classes $A(m, r)$, com $0 \leq r < m$.*

*Demonstração.* **a)** As classes são $A(m,0)$, $A(m,1)$, ..., $A(m,m-1)$. Para provar que são $m$ conjuntos, basta provar que se $r$ e $s$ são inteiros tais que $0 \leq r < s < m$, então $A(m,r)$ e $A(m,s)$ são diferentes. Notemos que $r \in A(m,r)$ mas $r \notin A(m,s)$. De fato, $r \in A(m,r)$ porque $r = 0 \cdot m + r \in A(m,r)$, por definição. Por outro lado, se ocorresse $r \in A(m,s)$ poderíamos escrever $r = qm + s$ para algum inteiro $q$. Mas então $m \mid s - r$, o que é impossível pois $0 < s - r < m$. Portanto $A(m,r)$ e $A(m,s)$ são diferentes. **b)** Com as notações acima, suponhamos que existisse $a \in A(m,r) \cap A(m,s)$. Então $a = qm + r$ e $a = tm + s$. Logo $qm + r = tm + s$, e novamente temos $m \mid s - r$, o que é impossível. Portanto $A(m,r)$ e $A(m,s)$ são disjuntos. **c)** De fato, dado $a \in \mathbb{Z}$, seja $a = qm + r$, para $0 \leq r < m$. Então $a \in A(m,r)$. □

As congruências, juntamente com o protocolo de Gauss, são extensamente utilizadas em Teoria dos Números. Para aprender mais consulte [24], [49], [71] e [108], dentre outros.

## 9.12 Problemas

**Problema 9.12.1.** Usando congruências, calcule o resto da divisão euclidiana de $3^{6n}$ por 13 para todo $n \geq 1$.

**Problema 9.12.2.** Usando congruências, demonstre que $3^{6n} - 2^{6n}$ é múltiplo de 35 para todo $n \geq 0$.

**Problema 9.12.3.** Usando congruências, calcule os dois últimos dígitos de $7^{7^{1000}}$.

**Problema 9.12.4.** Usando congruências, calcule o resto da divisão euclidiana por 7 do número $10^{10} + 10^{10^2} + \cdots + 10^{10^{10}}$.

**Problema 9.12.5.** Verifique a seguinte lei de cancelamento: se $p$ é primo e $p \nmid c$, então $ac \equiv bc \pmod{p} \Rightarrow a \equiv b \pmod{p}$, quaisquer que sejam os inteiros $a$, $b$ e $c$.

**Problema 9.12.6.** Verifique que os restos da divisão euclidiana dos números 0, $3^0$, $3^1$, $3^2$, ..., $3^{15}$ por 17 formam o conjunto completo dos resíduos (mod 17).

**Problema 9.12.7.** Resolva a equação modular

$$x \equiv 5 \pmod{7}, \quad x \in \mathbb{Z},$$

e distinga a menor solução positiva.

**Problema 9.12.8.** Resolva a equação modular linear

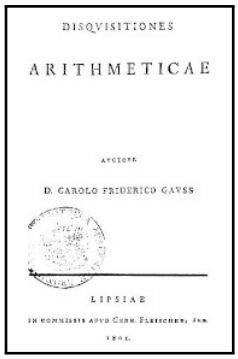
$$2x \equiv 3 \pmod{5}, \quad x \in \mathbb{Z},$$

e distinga a menor solução positiva.

**Problema 9.12.9.** Resolva a congruência quadrática

$$x^2 \equiv 4 \pmod{5}, \quad x \in \mathbb{Z},$$

e distinga a menor solução positiva.


DISQVISITIONES

ARITHMETICAE

AVCTORE

D. CAROLO FRIDERICO GAVSS

LIPSIAE

Figura 9.2. A figura ao lado é uma digitalização da capa da 1ª. edição do livro *Disquisitiones Arithmeticae* de Johann C. F. Gauss, publicada em 1801. A tradução do título em português pode ser "Investigações em Aritmética". O texto contém, dentre outros assuntos, congruência básica, resíduos de potências, congruências de primeiro e segundo grau, e aplicações. Inclui o teste de primalidade de Pierre de Fermat, o Teorema de Wilson, existência de raízes primitivas, lei da reciprocidade quadrática e formas quadráticas. Mais detalhes da digitalização na página 262.

# Capítulo 10

# O Método da Indução Completa

## 10.1 Introdução

Sabemos que as ciências naturais investigam os fenômenos utilizando métodos de indução e dedução. Já exploramos esses conceitos nos Problemas 4.2, em que vimos que a indução é uma operação que estabelece uma proposição geral com base no conhecimento de um certo número de dados particulares, e a dedução estabelece uma proposição geral com base em uma ou mais premissas com uma correta aplicação das regras da Lógica. Na Matemática, em particular, o método da indução é muito importante como processo de descoberta, mas preferimos a dedução como forma de verificar o conhecimento matemático na esperança de construir um corpo científico duradouro.

Surge então a questão de como podemos transformar uma propriedade obtida indutivamente em uma propriedade que passou pelo crivo da dedução. Vemos neste capítulo que, em situações matemáticas específicas, podemos usar para isso o chamado *Método da Indução Completa*, também conhecido por *Método da Indução Finita*.

## 10.2 Vale para 1, 2, 3, ..., $n$, vale sempre?

Sabemos, por experiência própria, que não. A História da Matemática relata exemplos de conjecturas gerais, propostas por matemáticos, usando observações particulares, mas depois essas conjecturas se mostraram incorretas. Um desses casos aconteceu com Pierre de Fermat, ilustre matemático do Século XVII. Ele observou que:

$2^{2^0}+1=2$ é primo;
$2^{2^1}+1=5$ é primo;
$2^{2^2}+1=17$ é primo;
$2^{2^3}+1=257$ é primo;
$2^{2^4}+1=65\,537$ é primo.

Baseando-se nesses fatos e em sua experiência em Teoria dos Números, Fermat aceitava que todos os números da forma $2^{2^n}+1$ seriam primos. Mas, no século seguinte, Leonard P. Euler mostrou que

$$2^{2^5}+1=4\,294\,967\,297=641\times 6\,700\,417$$

não é primo, contrariando a conjectura de Fermat. O estudante poderá verificar todas essas afirmações. Um método fácil para fazer isso é usar um aplicativo computacional algébrico.

## 10.3 Problemas

**Problema 10.3.1.** Gottfried Leibniz, eminente matemático do Século XVII, observou que:

$n^3 - n$ é múltiplo de 3 para todo número inteiro positivo $n$;
$n^5 - n$ é múltiplo de 5 "
$n^7 - n$ é múltiplo de 7 "

Dizem que, baseando-se nesses fatos, Leibniz supôs que $n^k - n$ seria múltiplo de $k$ para todo ímpar positivo $k$ e para todo número natural $n$. Mas ele mesmo descobriu um contra-exemplo. Demonstre as três afirmações acima e descubra você também um contra-exemplo para a conjectura.

**Problema 10.3.2.** Dmitry A. Grave, matemático russo, supôs que

(?) $2^{p-1} - 1$ não é múltiplo de $p^2$, para todo primo $p$.

De fato, essa afirmação é verdadeira para $p \leq 1091$. Mas, $2^{1092} - 1$ é múltiplo de $1093^2$, e 1093 é primo. O estudante pode usar um aplicativo computacional algébrico para verificar essa afirmação.

**Problema 10.3.3.** Quando se calcula a expressão $991n^2 + 1$ para $n = 1, 2, 3, \ldots$, não se encontra um quadrado de um número natural, mesmo se fizermos esse cálculo até $n = 12 \times 10^{27}$. Entretanto, não se pode concluir que $991n^2 + 1$ nunca é um quadrado perfeito. De fato, para

$$n = 12\,055\,735\,790\,331\,359\,447\,442\,538\,767,$$

a expressão $991n^2+1$ é um quadrado de um número inteiro, e esse é o menor $n$ para o qual ocorre esse fenômeno. O estudante poderá verificar essa afirmação fazendo um pequeno procedimento com um aplicativo computacional algébrico.

**Problema 10.3.4.** Confira as afirmações feitas no início da Seção 10.2 sobre os números de Fermat $2^{2^n} + 1$, $0 \leq n \leq 5$. E quanto a $n = 6$?

## 10.4 O Método da Indução Completa

Suponhamos que estejamos interessados em obter uma fórmula para $1+2+2^2+\ldots+2^n$, sendo $n$ um número natural qualquer. Uma fórmula talvez semelhante a $1+2+3+\ldots+n = n(n+1)/2$, a qual já conhecemos, e que nos permite calcular uma soma $1 + 2 + 3 + \ldots + n$ com valor de $n$ dado sem necessidade de adicionar os números um a um.

Para obter a fórmula desejada iniciamos com o método indutivo e observamos o que ocorre para $n = 0$, $n = 1$, $n = 2$, etc. Temos

$$\begin{aligned} 1 &= 1, \\ 1 + 2 &= 3, \\ 1 + 2 + 2^2 &= 7, \\ 1 + 2 + 2^2 + 2^3 &= 15. \end{aligned}$$

Se estivermos bem atentos e se esperamos encontrar uma fórmula envolvendo potências de 2, podemos observar que os resultados particulares obtidos são antecessores de potências de 2: $1 = 2^1 - 1$, $3 = 2^2 - 1$, $7 = 2^3 - 1$, $15 = 2^4 - 1$. Isso nos leva a induzir a seguinte generalização:

$$1 + 2 + 2^2 + 2^3 + \cdots + 2^n = 2^{n+1} - 1, \quad \text{para todo } n \in \mathbb{N}. \tag{10.1}$$

Essa propriedade, no momento, é uma conjectura. Não sabemos se é verdadeira para todo $n \in \mathbb{N}$, mas temos alguns motivos para crer que seja. Podemos aumentar essa crença examinando mais casos, $n = 4$, $n = 5$, etc. Podemos mesmo programar um computador e confirmar essa conjectura para milhares de casos, ou milhões, mas continuaremos com uma conjectura, sem a certeza que desejamos. Isso porque utilizamos um procedimento indutivo, e para reforçar nosso entendimento dessa situação a denominamos *indução incompleta*.

Para demonstrar a fórmula 10.1 necessitamos imaginar um argumento geral, que se aplica para todo número natural $n$. Por exemplo, podemos olhar $1 + 2 + 2^2 + 2^3 + \cdots + 2^n$ como a soma dos $n + 1$ primeiros termos de uma progressão geométrica de razão 2, e aplicar a fórmula que conhecemos para isso.

Por outro lado, para demonstrar a fórmula 10.1 podemos insistir no método inicial, o de conferi-la para todo $n \in \mathbb{N}$. Evidentemente esse é um projeto impossível, mas podemos imaginar uma forma de garantir que, mesmo não verificando para todo $n \in \mathbb{N}$, temos a certeza de que poderíamos fazê-lo, mesmo não tendo condições para isso.

A idéia é simples mas significativa. Dada uma afirmação $A(n)$, dependente de $n \in \mathbb{N}$, procedemos com os seguintes passos:

*Passo 1*: verificar a afirmação para $n = 0$. Em outros termos, verificar que $A(0)$ é verdadeira.

*Passo 2*: supor que a afirmação seja verdadeira para o número natural $n$ e demonstrar que isso implica que a afirmação é verdadeira para $n + 1$. Em outros termos, demonstrar a seguinte implicação para todo $n \in \mathbb{N}$:

$$A(n) \text{ verdadeira} \Rightarrow A(n+1) \text{ verdadeira}.$$

Tendo verificado essas duas propriedades para a afirmação $A(n)$, podemos perceber que ela é verdadeira para todo $n \in \mathbb{N}$. De fato, $A(0)$ é verdadeira devido ao passo 1. Aplicando agora o passo 2, vemos que $A(0) \Rightarrow A(0+1)$, portanto $A(1)$ é verdadeira. Aplicando novamente o passo 2, vemos que $A(1) \Rightarrow A(1+1)$, portanto $A(2)$ é verdadeira. E assim sucessivamente, podemos ver que $A(1000)$ é verdadeira, ou $A(n)$ é verdadeira para qualquer valor de $n$. Chamamos a esse método de *indução completa*.

Voltemos à nossa afirmação 10.1, denominando-a agora $A(n)$:

$$A(n): \quad 1 + 2 + 2^2 + 2^3 + \cdots + 2^n = 2^{n+1} - 1, \quad \text{para todo } n \in \mathbb{N}. \tag{10.2}$$

Vamos verificar que $A(n)$, com $n \geq 0$, satisfaz os passos 1 e 2 do método da indução completa.

Para $n = 0$ entendemos que $1 + 2 + 2^2 + 2^3 + \cdots + 2^n = 1$, e como $2^{n+1} - 1 = 1$ para $n = 0$, vemos que $A(0)$ é verdadeira. Esse é o passo 1 do método da indução completa.

Suponhamos agora que $A(n)$ seja verdadeira para algum número natural $n \geq 0$. Vamos verificar que isso implica que $A(n+1)$ é verdadeira. Temos como verdade que $1 + 2 + 2^2 + 2^3 + \cdots + 2^n = 2^{n+1} - 1$. Usamos isso em

$$\begin{aligned} 1+2+2^2+2^3+\cdots+2^{n+1} &= (1+2+2^2+2^3+\cdots+2^n)+2^{n+1} \\ &= (2^{n+1}-1)+2^{n+1} \\ &= 2\cdot 2^{n+1}-1 \\ &= 2^{n+2}-1. \end{aligned}$$

Demonstramos assim que $1+2+2^2+2^3+\cdots+2^{n+1}=2^{n+2}-1$, o que nada mais é do que a validade da afirmação $A(n+1)$. Fica assim visto que $A(n)$ verdadeira $\Rightarrow$ $A(n+1)$ verdadeira, que é o passo 2 do método da indução completa.

Concluímos que $A(n)$ é verdadeira para todo $n \in \mathbb{N}$.

Observamos que frequentemente uma afirmação $A(n)$ pode não ser verdadeira para alguns números naturais $n$. Por exemplo, a desigualdade $2^n < n!$ é falsa para $n = 0$, 1, 2 e 3. Mas constatamos que é verdadeira para $n = 4$, 5, 6 e 7. Isso nos leva a considerar a afirmação

$$A(n): \quad 2^n < n! \quad \text{para todo } n \geq 4 \text{ em } \mathbb{N}. \tag{10.3}$$

Para demonstrar essa afirmação usando o método da indução completa podemos adaptar a forma anterior para a seguinte, em que $n_0$ é um número natural dado:

*Passo 1*: verificar a afirmação para $n = n_0$. Em outros termos, verificar que $A(n_0)$ é verdadeira.

*Passo 2*: supor que a afirmação seja verdadeira para algum número natural $n \geq n_0$ e demonstrar que isso implica que a afirmação é verdadeira para $n+1$. Em outros termos, demonstrar a seguinte implicação: $A(n) \Rightarrow A(n+1)$ para todo $n \geq n_0$ em $\mathbb{N}$.

Tendo verificado esses dois passos para a afirmação $A(n)$, podemos perceber que ela é verdadeira para todo $n \geq n_0$ em $\mathbb{N}$.

Vamos conferir se a afirmação 10.3 é verdadeira verificando esses dois passos com $n_0 = 4$. Como $2^4 < 4!$, vemos que o passo 1 está correto. Suponhamos agora que 10.3 seja verdadeira para algum número natural $n \geq 4$. Temos assim $2^n < n!$ Notemos que $2^{n+1} = 2 \cdot 2^n < 2 \cdot n! < (n+1)n! = (n+1)!$, pois $n \geq 4$ implica $n+1 > 2$. Provamos que $A(n) \Rightarrow A(n+1)$ para todo $n \geq n_0$ em $\mathbb{N}$, e portanto o passo 2 está verificado. Concluímos que $2^n < n!$ para todo $n \geq 4$ em $\mathbb{N}$.

**Problema resolvido 10.1.** Demonstre que $1+2+3+\cdots+n = \frac{n(n+1)}{2}$ para todo inteiro $n \geq 1$ usando o método da indução completa.

*Solução.*
*Passo 1*: verificar a afirmação para $n = 1$.

Para $n = 1$, a afirmação diz que

$$1 = \frac{1(1+1)}{2}$$

o que é verdadeiro.

*Passo 2*: supor que a afirmação seja verdadeira para o número natural $n \geq 1$ e demonstrar que isso implica que a afirmação é verdadeira para $n+1$. Isso equivale a supor ser verdadeiro que

$$1+2+3+\cdots+n = \frac{n(n+1)}{2}, \tag{$*$}$$

e deve ser verificado que

$$1+2+3+\cdots+(n+1)=\frac{(n+1)(n+2)}{2}. \qquad (**)$$

Para demonstrar $(**)$ a partir de $(*)$ procedemos assim:

$$\begin{aligned} 1+2+3+\cdots+(n+1) &= (1+2+3+\cdots+n)+(n+1) \\ &= \frac{n(n+1)}{2}+(n+1) \quad \text{(devido a } (*)\text{)} \\ &= \frac{n(n+1)+2(n+1)}{2} \\ &= \frac{(n+1)(n+2)}{2} \end{aligned}$$

e fica provado $(**)$.

Em virtude do método da indução completa a afirmação está provada para todo número natural $n \geq 1$. □

**Problema resolvido 10.2.** Demonstre, usando o método da indução completa, que a soma dos $n$ primeiros números ímpares positivos é igual a $n^2$.

*Solução.* De fato,

$$\begin{aligned} 1 &= 1^2; \\ 1+3 &= 4=2^2; \\ 1+3+5 &= 9=3^2; \\ 1+3+5+7 &= 16=4^2; \\ 1+3+5+7+9 &= 25=5^2. \end{aligned}$$

Esses eventos nos sugerem

$$1+3+5+\cdots+(2n-1)=n^2 \quad \text{para todo } n \geq 1 \text{ em } \mathbb{N}. \qquad (10.4)$$

Vamos chamar essa afirmação de $A(n)$, e verificar os dois passos do método da indução completa.

*Passo 1*: provar a afirmação $A(1)$.

O primeiro número ímpar é 1, e $1=1^2$. Portanto, $A(1)$ é verdadeira.

*Passo 2*: provar que se $A(n)$ é verdadeira então $A(n+1)$ é verdadeira. Em outros termos, vamos supor que

$$1+3+5+\cdots+(2n-1)=n^2 \qquad (*)$$

seja verdadeiro e provar que

$$1+3+5+\cdots+(2n+1)=(n+1)^2. \qquad (**)$$

Notemos que

$$\begin{aligned} 1+3+5+\cdots+(2n+1) &= 1+3+5+\cdots+(2n-1)+(2n+1) \\ &= n^2+2n+1 \quad \text{(devido a } (*)\text{)} \\ &= (n+1)^2. \end{aligned}$$

Portanto, $(*)$ implica $(**)$, e com isso fica estabelecido o passo 2 da indução completa. Podemos concluir que é verdadeira a afirmação 10.4. □

Segundo Proclus Diadochus, filósofo, matemático e historiador do Século V, o método da indução completa era essencialmente conhecido pela Escola Pitagórica. O primeiro escritor a utilizar explicitamente o método foi Francisco Maurolico, em sua obra *Arithmetica*, de 1575. Blaise Pascal, por volta de 1653, usou o método para demonstrar uma propriedade do triângulo aritmético, hoje chamado triângulo de Pascal, em sua homenagem. A forma adotada por Pascal está bem próxima da que é utilizada nos dias atuais.

No método da indução completa o passo 1 chama-se *base da indução*. No passo 2 a afirmação "$A(n)$ é verdadeira" chama-se *hipótese da indução*, e a afirmação "$A(n+1)$ é verdadeira" chama-se *tese da indução*. Se for conveniente a condição $A(n) \Rightarrow A(n+1)$ pode ser substituída por $A(n-1) \Rightarrow A(n)$, ou outra forma equivalente.

## 10.5 Problemas

**Problema 10.5.1.** Desmonstre que $1+2+2^2+2^3+\cdots+2^n = 2^{n+1}-1$ para todo número natural $n$ usando a fórmula da soma dos termos de uma progressão geométrica. Procure essa fórmula em algum livro texto, e observe se, para obter a fórmula, o autor usou indução ou dedução.

**Problema 10.5.2.** Observe que

$$\begin{aligned} 1 &< 2 \\ 2 &< 2^2 \\ 3 &< 2^3, \quad \text{etc.} \end{aligned}$$

Extraia daí uma afirmação $A(n)$, e demonstre-a pelo método da indução completa.

**Problema 10.5.3.** A partir dos experimentos

$$\begin{aligned} \frac{1}{1\cdot 2} &= \frac{1}{2}, \\ \frac{1}{1\cdot 2}+\frac{1}{2\cdot 3} &= \frac{2}{3}, \\ \frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4} &= \frac{3}{4}, \end{aligned}$$

induza uma fórmula geral para a soma

$$\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}+\cdots+\frac{1}{n(n+1)}$$

para todo $n \geq 1$. Demonstre a fórmula pelo método da indução completa.

**Problema 10.5.4.** Deduza uma fórmula para o produto

$$\left(1+\frac{1}{1}\right)\left(1+\frac{1}{2}\right)\left(1+\frac{1}{3}\right)\cdots\left(1+\frac{1}{n}\right)$$

para todo $n \geq 1$.

**Problema 10.5.5.** Deduza uma fórmula para o produto

$$\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{4}\right)\cdots\left(1-\frac{1}{n}\right)$$

para todo $n \geq 2$.

**Problema 10.5.6.** Prove que

$$1^2+2^2+3^2+\cdots+n^2=\frac{n(n+1)(2n+1)}{6}$$

para todo $n \geq 1$.

**Problema 10.5.7.** Demonstre que

$$1^3+3^3+5^3+\cdots+(2n-1)^3=n^2(2n^2-1)$$

para todo $n \geq 1$.

**Problema 10.5.8.** Prove que

$$\frac{1}{1\cdot 2\cdot 3}+\frac{1}{2\cdot 3\cdot 4}+\cdots+\frac{1}{n(n+1)(n+2)}=\frac{n(n+3)}{4(n+1)(n+2)}$$

para todo $n \geq 1$.

**Problema 10.5.9.** Em uma festa com $n$ pessoas, cada uma cumprimentou com um aperto de mão cada uma das outras. Encontre fórmulas para o número de cumprimentos. Você precisou, para justificar, do Método da Indução Completa?

## 10.6 O segundo princípio da Indução Completa

Nas seções anteriores fizemos uma apresentação informal do método da indução completa. Para prosseguir necessitamos de uma apresentação mais formal. Vejamos duas formulações do método, a primeira já é conhecida, mas tem a diferença de que o número de partida $n_0$ pode ser negativo.

**Primeiro Princípio da Indução Completa.** Seja $n_0$ um número inteiro e seja $A(n)$ uma afirmação associada a todo número inteiro $n \geq n_0$. Suponhamos que sejam válidas as seguintes propriedades:
**a)** $A(n_0)$ é verdadeira;
**b)** para todo número inteiro $n \geq n_0$, se $A(n)$ é verdadeira então $A(n+1)$ é verdadeira.
Nessas condições, $A(n)$ é verdadeira para todo número inteiro $n \geq n_0$.

O método descrito acima é uma consequência direta do Princípio de Indução apresentado na página 198. De fato, seja $V$ o conjunto dos números inteiros $n \geq n_0$ para os quais $A(n)$ é verdadeira. Consideremos o conjunto $S = V - n_0 = \{m - n_0 \mid m \in V\}$. Temos $S \subseteq \mathbb{N}$. Como $n_0 \in V$ temos $0 \in S$, portanto está satisfeita a condição (i) do Princípio de Indução. Seja $n \in S$. Então $n = m - n_0$ para algum $m \in V$. Em virtude da condição b) acima temos $m+1 \in V$. Logo $n+1 = (m+1) - n_0 \in S$. Portanto está satisfeita a condição (ii) do Princípio de Indução, do que segue que $S = \mathbb{N}$. Seja agora um inteiro qualquer $n \geq n_0$. Como $n - n_0 \in \mathbb{N}$ temos $n - n_0 \in S$ o que implica $n \in V$. Isso termina a demonstração.

A segunda formulação do método é equivalente à primeira mas nos permite lidar mais facilmente com certos tipos de afirmações recorrentes.

**Segundo Princípio da Indução Completa.** Seja $n_0$ um número inteiro e seja $A(n)$ uma afirmação associada a todo número inteiro $n \geq n_0$. Suponhamos que sejam válidas as seguintes propriedades:
**a)** $A(n_0)$ é verdadeira;
**b)** para todo número inteiro $n \geq n_0$, se $A(r)$ é verdadeira para todo número inteiro $r$ tal que $n_0 \leq r \leq n$ então $A(n+1)$ é verdadeira.

Nessas condições, $A(n)$ é verdadeira para todo número inteiro $n \geq n_0$.

Uma forma de demonstrar esse método consiste em utilizar o Teorema 9.7. Seja $V = \{n \in \mathbb{Z} \mid n \geq n_0 \text{ e } A(n) \text{ é verdadeira}\}$. Queremos provar que $V = \{n \in \mathbb{Z} \mid n \geq n_0\}$. Suponhamos que sejam diferentes. Então é não vazio e limitado inferiormente o conjunto $A = \{n \in \mathbb{Z} \mid n \geq n_0\} - V$. Seja $m$ o mínimo de $A$. Consideremos o número $n = m - 1$. Temos $n_0 \in V \Rightarrow n_0 \notin A \Rightarrow m > n_0 \Rightarrow m - 1 \geq n_0 \Rightarrow n \geq n_0$. Para todo inteiro $r$ tal que $n_0 \leq r \leq n$ temos $r \notin A \Rightarrow r \in V$. Em virtude da condição b) acima $m \in V$. Mas então $m \notin A$, o que é uma contradição.

Vejamos dois exemplos de aplicação do Segundo Princípio da Indução Completa. Definimos a *sequência de Fibonacci* $(f_n)_{n\geq 0}$ por

$$\begin{cases} f_0 &= 0, \quad f_1 = 1, \\ f_n &= f_{n-1} + f_{n-2}, \quad n \geq 2. \end{cases} \tag{10.5}$$

Portanto a sequência $(f_n)_{n\geq 0}$ é constituída pelos números 0, 1, 1, 2, 3, 5, 8, 13, ..., cada número é a soma dos dois anteriores.

**Problema resolvido 10.3.** Prove que todo número natural é um número de Fibonacci ou pode ser representado como a soma de números de Fibonacci diferentes dois a dois.

*Solução.* Consideremos a afirmação $A(n)$:

"Todo número natural $n$ é um número de Fibonacci ou é a soma de números de Fibonacci diferentes dois a dois."

Vamos provar que $A(n)$ é verdadeira para todo inteiro $n \geq 0$ usando o Segundo Princípio da Indução Completa.

Observemos que $A(0)$ é verdadeira, pois para $n = 0$ temos $0 = f(0)$. Ainda, $A(1)$ também é verdadeira pois para $n = 1$ temos $1 = f(1)$.

Seja $n \geq 1$ um número inteiro, e suponhamos que $A(r)$ seja verdadeira para todo número inteiro $r$ tal que $1 \leq r \leq n$. Vamos provar que $A(n+1)$ é verdadeira. Como os números de Fibonacci formam uma sequência crescente, existe um número inteiro $m$ tal que $f_m \leq n+1 < f_{m+1}$. Temos $f_m \geq 2$ e $m \geq 3$. Se $n + 1 = f_m$, terminamos. Suponhamos que $f_m < n + 1$, e

consideremos a diferença $r = n + 1 - f_m$. Como $1 \leq r \leq n$ temos que $A(r)$ é verdadeira, e assim $r$ se escreve na forma

$$r = f_{i_1} + f_{i_2} + \ldots + f_{i_s},$$

em que $f_{i_1} < f_{i_2} < \ldots < f_{i_s}$. Nesse caso $n + 1 = r + f_m = f_{i_1} + f_{i_2} + \ldots + f_{i_s} + f_m$. Para terminar basta provar que $f_{i_s} \neq f_m$. Afirmamos que $f_{i_s} < f_m$. Se fosse $f_{i_s} \geq f_m$ teríamos $n + 1 = f_m + r \geq f_m + f_{i_s} \geq f_m + f_m > f_m + f_{m-1} = f_{m+1}$, o que é uma contradição. Fica provado que $A(n + 1)$ é verdadeira.

Em virtude do Segundo Princípio da Indução Completa a afirmação $A(n)$ é verdadeira para todo $n \geq 0$. □

**Problema resolvido 10.4.** Todo número natural $\geq 2$ é primo ou se escreve como produto de primos.

*Solução.* Esse resultado já foi demonstrado no Teorema 4.22. Apresentamos outra demonstração usando o Segundo Princípio da Indução Completa.

Consideremos a afirmação $A(n)$:

"$n$ é primo ou se escreve como produto de primos."

Observemos que $A(2)$ é verdadeira, pois 2 é primo. Seja $n \geq 2$ um inteiro e suponhamos que $A(r)$ seja verdadeira para todo $r$ tal que $2 \leq r \leq n$. Vamos provar que $A(n + 1)$ é verdadeira. Se $n + 1$ é primo, terminamos. Suponhamos que $n + 1$ não seja primo. Então existem inteiros positivos $a$ e $b$ tais que $n + 1 = ab$, $2 \leq a < n + 1$ e $2 \leq b < n + 1$. Portanto $A(a)$ e $A(b)$ são verdadeiras e $a$ e $b$ são primos ou produto de primos. Mas então $n+1$ é um produto de primos. Assim $A(n + 1)$ é verdadeira.

Em virtude do Segundo Princípio da Indução Completa a afirmação $A(n)$ é verdadeira para todo $n \geq 2$. □



Figura 10.1. Leonardo de Pisa, mais conhecido como Fibonacci, é reconhecido como o primeiro grande matemático da Idade Média. Contribuiu com o renascimento das ciências exatas na Europa, depois de 1000 anos de abandono. Seu pai era mercador, o que lhe deu oportunidade de conhecer a aritmética praticada na Índia e pelos povos muçulmanos. Em 1202, aos 32 anos, publicou o *Liber Abaci*, em que introduziu na Europa o sistema decimal com os numerais hindu-arábicos. Ao lado, monumento dedicado a Fibonacci em Pisa, Itália. Mais detalhes na página 262.

## 10.7 Problemas

**Problema 10.7.1.** Prove que dois termos consecutivos quaisquer da sequência de Fibonacci são relativamente primos.

**Problema 10.7.2.** Demonstre a seguinte afirmação a respeito da sequência de Fibonacci $(f_n)_{n\geq 0}$: $f_n$ é múltiplo de 3 sempre que $n$ é múltiplo de 4.

**Problema 10.7.3.** Demonstre, usando o Segundo Princípio da Indução Completa, que os números de Fibonacci podem ser expressos pela seguinte fórmula:

$$f_n = \frac{1}{\sqrt{5}} \left[ \left( \frac{1+\sqrt{5}}{2} \right)^n - \left( \frac{1-\sqrt{5}}{2} \right)^n \right], \; n \geq 0.$$

**Problema 10.7.4.** A *sequência de Lucas* $(l_n)_{n\geq 1}$ é definida por

$$\begin{cases} \ell_1 &= 1, \quad \ell_2 = 3, \\ \ell_n &= \ell_{n-1} + \ell_{n-2}, \quad n \geq 3. \end{cases} \tag{10.6}$$

Demonstre que

$$\ell_n = \alpha^n + \beta^n, \quad n \geq 1,$$

sendo $\alpha = \big(1+\sqrt{5}\big)/2$ e $\beta = \big(1-\sqrt{5}\big)/2$.

**Problema 10.7.5.** Demonstre o seguinte resultado sobre a sequência de Lucas: $l_n < (7/4)^n$, $n \geq 1$.

## 10.8 Problemas adicionais

**Problema 10.8.1.** Já vimos os números binomiais $\binom{n}{i} = \frac{n!}{i!(n-i)!}$ sendo $0 \leq i \leq n$ naturais. Esses números são inteiros, pois medem a quantidade de subconjuntos com $i$ elementos de um conjunto com $n$ elementos. **a)** Verifique a relação de recorrência binomial: para todo $n \geq 2$ e $0 < i < n$ vale que $\binom{n-1}{i-1} + \binom{n-1}{i} = \binom{n}{i}$. **b)** Usando o método da indução completa demonstre a fórmula do binômio

$$(x+y)^n = x^n + \binom{n}{1}x^{n-1}y + \binom{n}{2}x^{n-2}y^2 + \ldots + \binom{n}{n-1}xy^{n-1} + y^n$$

quaisquer que sejam os números reais $x$ e $y$ e o número natural $n \geq 1$. **c)** Usando o método da indução completa mostre diretamente que todo número binomial é inteiro.

**Problema 10.8.2.** Retome o Problema 4.2.2 e demonstre-o usando o método da indução completa.

**Problema 10.8.3.** Prove que $3^{2n} - 1$ é múltiplo de 8 para todo número natural $n$.

**Problema 10.8.4.** Prove que $n^3 + 2n$ é múltiplo de 3 para todo número natural $n \geq 1$.

**Problema 10.8.5.** Prove que todo polígono convexo com $n \geq 3$ lados tem $n(n-3)/2$ diagonais.

**Problema 10.8.6.** Use o método da indução completa para verificar que

$$(1+a)(1+a^2)(1+a^4)\cdots(1+a^{2^n}) = \frac{a^{2^{n+1}}-1}{a-1}, \quad n \geq 0,$$

para todo número real $a \neq 1$.

**Problema 10.8.7.** Demonstre, pelo método da indução completa, as desigualdades

$$n^2 < n!, \quad n \geq 4;$$

$$n^3 < n!, \quad n \geq 6;$$

$$n^2 < 2^n, \quad n \geq 5;$$

$$\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \cdots + \frac{1}{\sqrt{n}} > \sqrt{n}, \quad n \geq 2.$$

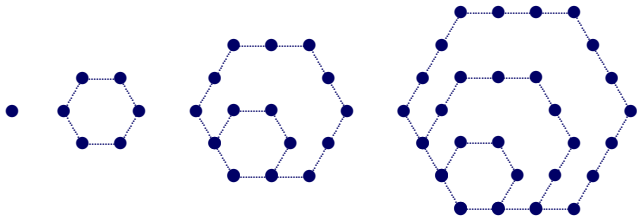
**Problema 10.8.8.** Demonstre, pelo método da indução completa, que

$$1(1!) + 2(2!) + 3(3!) + \cdots + n(n!) = (n+1)! - 1, \quad n \geq 1.$$

**Problema 10.8.9.** Demonstre, pelo método da indução completa, o Pequeno Teorema de Fermat, já apresentado no Teorema 9.18:

se $p$ é primo então $p|(a^p - a)$ para todo inteiro $a$.

**Problema 10.8.10.** Considere a sequência das figuras hexagonais:



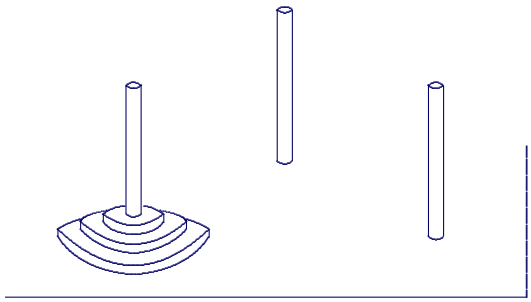
Observando a lei de formação dessas figuras, obtemos a seguinte definição por recorrência dos números hexagonais:

$$\begin{cases} H_1 &= 1, \\ H_n &= H_{n-1} + 4n - 3, \quad n \geq 2. \end{cases} \tag{10.7}$$

Demonstre, pelo método da indução completa, que

$$H_n = \frac{n(4n-2)}{2}, \quad n \geq 1.$$

**Problema 10.8.11.** Um jogo chamado *Torre de Hanoi*, inventado pelo matemático francês Edouard Lucas, consiste de três bastões fixados verticalmente em uma base, e $n$ discos de raios diferentes, perfurados no centro, de modo que possam ser colocados nos bastões.



O jogo começa com os $n$ discos colocados em um bastão, dispostos, de baixo para cima, em ordem decrescente de tamanho. Todos os discos devem ser transferidos para um dos outros bastões. O terceiro bastão pode ser utilizado como passagem. O movimento permitido é tirar o disco superior de um bastão e colocá-lo em outro, desde que não sobre um disco menor.

Seja $m_n$ o menor número de movimentos necessários para transferir $n$ discos de um bastão para outro. Observe que $m_1 = 1$, $m_2 = 3$, $m_3 = 7$ e $m_4 = 15$. Demonstre que $m_n = 2^n - 1$ para todo $n \geq 1$.

"Conta-se" que, em um mosteiro na Índia, os monges se revezam na tarefa de transferir 64 discos de ouro, obedecendo às regras do jogo. Fazem-no desde o começo do mundo, à razão de um disco por segundo. Diz a "lenda" que, quando os monges terminarem seu trabalho, o mundo acabará. Supondo que o mundo foi criado há 4 bilhões de anos, calcule por quanto tempo ele ainda existirá.

**Problema 10.8.12.** Ao usar o método da indução completa, o estudante inexperiente pode julgar sem importância a verificação da primeira parte do método. Os seguintes exemplos irão convencê-lo do contrário.

Todas as afirmações abaixo são falsas. Verifique, em cada caso, que a segunda parte do método da indução completa pode ser demonstrada.

(FALSO) $1 + 3 + 5 + \cdots + (2n - 1) = n^2 + 3, \quad n \geq 1;$

(FALSO) $n^2 + n$ é ímpar para todo $n$;

(FALSO) $n = n + 1$ para todo número natural $n$, isto é, todos os números naturais são iguais.

**Problema 10.8.13.** Considere a afirmação obviamente falsa: "$n$ elementos quaisquer são iguais dois a dois, para todo número natural $n \geq 1$". Descubra o erro da seguinte "demonstração":

"É claro que essa afirmação vale para $n = 1$. Vamos mostrar que se a afirmação vale para $n$ então vale para $n+1$. Consideremos $n+1$ elementos $a_1$, $a_2$, $a_3$, ..., $a_{n+1}$. Então os $n$ elementos $a_1$, $a_2$, ..., $a_n$ são iguais dois a dois, devido à hipótese da indução. Pelo mesmo motivo são iguais dois a dois os $n$ elementos $a_2$, $a_3$, ..., $a_{n+1}$. Mas então os $n + 1$ elementos $a_1$, $a_2$, $a_3$, ..., $a_{n+1}$ são iguais dois a dois."

O que está errado?

**Problema 10.8.14.** A fórmula para $f_n$ apresentada no Problema 10.7.3 foi observada pelo matemático Abraham De Moivre em 1718. Vejamos como essa fórmula foi "achada".

Sejam $\alpha$ e $\beta$ as raízes da equação $x^2 = x + 1$. Portanto $\alpha^2 = \alpha + 1$ e $\beta^2 = \beta + 1$. Multiplicando essas igualdades por $\alpha^{n-2}$ e $\beta^{n-2}$ respectivamente, obtemos $\alpha^n = \alpha^{n-1} + \alpha^{n-2}$ e $\beta^n = \beta^{n-1} + \beta^{n-2}$ para todo $n \geq 2$. Assim as potências $\alpha^n$ e $\beta^n$ obedecem à mesma lei de recorrência da sequência de Fibonacci. Por isso $x^2 = x + 1$ chama-se *equação característica* dessa lei de recorrência, e a experiência sugere que $f_n$ é uma combinação linear de $\alpha^n$ e $\beta^n$, isto é, existem números reais $A$ e $B$ tais que

$$f_n = A\alpha^n + B\beta^n \text{ para todo } n \geq 0. \tag{10.8}$$

**a)** Mostre que existem números $A$ e $B$ tais que a relação (10.8) vale para $n = 0$ e $n = 1$. **b)** Demonstre (10.8) para todo $n \geq 0$. **c)** Observe que é a mesma fórmula do Problema 10.7.3.

**Problema 10.8.15.** E. Lucas descobriu em 1876 que os números de Fibonacci podem ser escritos na forma

$$f_n = \binom{n-1}{0} + \binom{n-2}{1} + \binom{n-3}{2} + \cdots + \binom{n-j}{j-1} + \binom{n-j-1}{j}, \; n \geq 1,$$

sendo $j$ é o maior inteiro menor ou igual a $(n-1)/2$. Essa fórmula pode ser demonstrada através do método da indução completa.

## 10.9 Temas para investigação

**Tema 10.9.1. a)** Vimos no Problema 10.8.7 que $n^2 < n!$ para todo $n \geq 4$ e que $n^3 < n!$ para todo $n \geq 6$. Verifique se existe um número natural $n_0$ tal que $n^4 < n!$ para todo $n \geq n_0$. Investigue alguma possível generalização. **b)** Demonstre que $2^n < n!$ para todo $n \geq 4$ e que

$3^n < n!$ para todo $n \geq 7$. Verifique se existe um número natural $n_0$ tal que $4^n < n!$ para todo $n \geq n_0$. Investigue alguma possível generalização. **c)** Vimos no Problema 10.8.7 que $n^2 < 2^n$ para todo $n \geq 5$. Investigue alguma possível generalização. **d)** Examine a distância entre $2^n$ e $n!$ e verifique que ela aumenta consideravelmente à medida que $n$ cresce. Portanto $2^n$ não é uma boa aproximação de $n!$ Investigue uma aproximação melhor.

**Tema 10.9.2.** Investigue regularidades e fórmulas relativas à sequência de Fibonacci. Por exemplo, encontre (e justifique) uma fórmula para a soma dos $n$ primeiros termos da sequência.

**Tema 10.9.3.** No início da Seção 10.2, assim como no Problema 10.3.4, vimos o que são os números de Fermat $2^{2^n}+1$. Investigue regularidades sobre esses números. Para ajudar, temos abaixo uma tabela com os valores de alguns deles e sua decomposição canônica:

| $n$ | valor de $2^{2^n}+1$ | decomposição em primos |
|---|---|---|
| 0 | 2 | 2 (primo) |
| 1 | 5 | 5 (primo) |
| 2 | 17 | 17 (primo) |
| 3 | 257 | 257 (primo) |
| 4 | 65537 | 65537 (primo) |
| 5 | 4294967297 | $641 \cdot 6700417$ |
| 6 | 18446744073709551617 | $274177 \cdot 67280421310721$ |
| 7 | 340282366920938463463374607431768211457 | $59649589127497217 \cdot 5704689200685129054721$ |



Figura 10.2. François E. A. Lucas, geralmente referido como Édouard Lucas, foi um matemático francês, tendo trabalhado como professor em escolas de Paris. Contribuiu especialmente em Teoria dos Números. É conhecido pela *sequência de Lucas* e por *testes de primaridade*. Gostava de matemática recreativa, e inventou o jogo *Torre de Hanoi*, que chegou a comercializar. Ao lado, foto de É. Lucas. Mais detalhes na página 262.

# Capítulo 11

# A equação ax + by = c em $\mathbb{Z}$

## 11.1 Introdução

Sejam $a$, $b$ e $c$ números inteiros com $a \neq 0$ e $b \neq 0$. A equação

$$ax + by = c, \quad \text{com } x, y \in \mathbb{Z}, \tag{11.1}$$

chama-se *equação diofantina linear a duas incógnitas*. A literatura utiliza esse nome em homenagem ao matemático grego Diofanto de Alexandria, devido à ênfase que ele deu às equações com soluções inteiras ou racionais em seu livro *Arithmetica*, escrito no Século III.

Os hindus utilizavam equações diofantinas lineares para calcular períodos astronômicos. Encontravam as soluções através de um algoritmo denominado *kuttaka*, que descrevemos aqui. Apresentamos também um método algébrico que inclui uma fórmula que fornece todas as soluções.

As equações diofantinas lineares têm diversas aplicações na Matemática. Neste texto vemos alguns problemas em que elas aparecem, e que o estudante certamente achará interessantes.

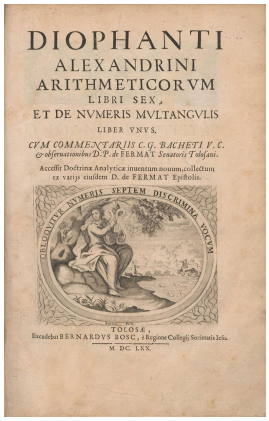

DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX,
ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.
CVM COMMENTARIIS C. G. BACHETI V. C.
& observationibus D. P. de FERMAT Senatoris Tolosani.
Accessit Doctrina Analytica inuentum nouum, collectum
ex variis eiusdem D. de FERMAT Epistolis.
TOLOSÆ,
M. DC. LXX.

Figura 11.1. Diofanto de Alexandria estudou e trabalhou na Escola de Alexandria, e foi um dos mais importantes matemáticos clássicos da Antiga Grécia. A maioria de seus escritos foram perdidos, mas *Arithmetica* foi, em boa parte, preservado, e os assuntos ali tratados foram extensivamente estudados por matemáticos posteriores. Trata-se de uma coletânea de problemas algébricos, principalmente equações indeterminadas com coeficientes inteiros. Diofanto mostrou grande inventividade nas ideias e nas notações, sendo considerado, por esse trabalho, o Pai da Álgebra. Ao lado, capa de uma edição latina do livro *Arithmetica* (mais detalhes na página 262).

## 11.2 Exemplos iniciais

"De quantas maneiras pode o encarregado do caixa de um banco pagar a um cliente a quantia de R$ 1000,00 em notas de R$ 10,00 e R$ 50,00?" Se $x$ é a quantidade de notas de R$ 10,00 e $y$ a de R$ 50,00, queremos resolver a equação

$$10x + 50y = 1000, \quad \text{com } x, y \in \mathbb{N}. \tag{11.2}$$

Simplificando $10x+50y = 1000$ por 10 temos $x+5y = 100$. Tomando $y = t$ como parâmetro vem $x = 100 - 5t$. Portanto as soluções são $(x, y) = (100 - 5t, t)$ com $t \in \mathbb{Z}$. Mas queremos soluções com $x \geq 0$ e $y \geq 0$. Notemos que $x \geq 0 \iff t \leq 20$ e $y \geq 0 \iff t \geq 0$. Encontramos assim 21 soluções, dadas por $(x, y) = (100 - 5t, t)$ com $t \in \mathbb{Z}$ e $0 \leq t \leq 20$.

Vimos um exemplo de equação diofantina linear que tem infinitas soluções. Mas pode ocorrer outra situação. Notemos que a equação $21x + 9y = 5$ não tem solução para $x, y \in \mathbb{Z}$. De fato, se existissem $x_0, y_0 \in \mathbb{Z}$ tais que $21x_0 + 9y_0 = 5$, teríamos $3 \mid 21x_0 + 9y_0$, mas $3 \nmid 5$, o que seria uma contradição.

Assim, uma primeira observação de caráter geral é que se $ax + by = c$ tem solução com $x, y \in \mathbb{Z}$, então todo divisor comum de $a$ e $b$ é também divisor de $c$. Dessa forma uma condição necessária para que existam soluções é que $\text{mdc}(a, b) \mid c$. Veremos que essa condição é também suficiente para que exista solução.

Notamos algumas situações particulares em que é fácil resolver 11.1. Se $a = 1$, tomamos $y = t$ como parâmetro, e as soluções de $x + by = c$ são dadas por $(x, y) = (c - bt, t)$, para todo $t \in \mathbb{Z}$. Se $b = 1$, tomamos $x = t$ como parâmetro, e as soluções de $ax + y = c$ são dadas por $(x, y) = (t, c - at)$, para todo $t \in \mathbb{Z}$.

Outra situação particular ocorre se $a = b$ na equação 11.1. Temos $a(x + y) = c$, que tem solução se e somente se $a \mid c$. Nesse caso $\frac{c}{a} \in \mathbb{Z}$, e a equação equivale a $x + y = \frac{c}{a}$. Tomando $y = t$ como parâmetro, as soluções são $(x, y) = (\frac{c}{a} - t, t)$, para todo $t \in \mathbb{Z}$.

Um exemplo que não se encaixa nos casos anteriores é $3x + 5y = 2$. A idéia é manipular essa equação e expressá-la em uma das formas anteriores. Notando que $3x + 5y = 2 \iff 3(x + y) + 2y = 2$, introduzimos a variável $z = x + y$, e obtemos $3z + 2y = 2$. De modo similar observamos que $3z + 2y = 2 \iff z + 2(z + y) = 2$. Definimos a variável $w = z + y$, e obtemos $z + 2w = 2$. Essa última equação é do tipo desejado.

Esse processo nos deu três sistemas equivalentes:

$$3x + 5y = 2 \iff \begin{cases} 3z + 2y &= 2 \\ x + y &= z \end{cases} \iff \begin{cases} z + 2w &= 2 \\ x + y &= z \\ z + y &= w \end{cases}$$

Tomando $w = t$ como parâmetro, as soluções de $z + 2w = 2$ são $(z, w) = (2 - 2t, t)$, para todo $t \in \mathbb{Z}$. Então $y = w - z = t - (2 - 2t) = 3t - 2$ e $x = z - y = 2 - 2t - (3t - 2) = -5t + 4$. Obtivemos assim o conjunto solução de $3x + 5y = 2$, a saber, $(x, y) = (-5t + 4, 3t - 2)$ para todo $t \in \mathbb{Z}$.

## 11.3 O método da pulverização

Para resolver a equação $9x+2y = 5$ utilizando o processo descrito no final da seção anterior, temos que aplicar vários passos, fazendo $9-2 = 7$, $7-2 = 5$, $5-2 = 3$, $3-2 = 1$. São subtrações sucessivas. Isso nos indica que podemos economizar alguns passos se considerarmos a divisão de 9 por 2. Como $9 = 4 \cdot 2 + 1$, temos $9x + 2y = 5 \iff (4 \cdot 2 + 1)x + 2y = 5 \iff x+2(4x+y) = 5$. Pondo $z = 4x+y$ temos a equação equivalente $x+2z = 5$, cujas soluções são $z = t$ e $x = 5 - 2t$. Portanto $y = z - 4x = t - 4(5 - 2t) = 9t - 20$, e as soluções de $9x + 2y = 5$ com $x, y \in \mathbb{Z}$ são $(x, y) = (5 - 2t, 9t - 20)$ para todo $t \in \mathbb{Z}$.

Em geral, dada $ax + by = c$ com $a, b, c \in \mathbb{Z}$ tais que $\text{mdc}(a, b) \mid c$, podemos encontrar seu conjunto solução para $x, y \in \mathbb{Z}$ utilizando o procedimento descrito acima. Para mais detalhes confira o Problema 11.5.10. Esse é o chamado algoritmo *kuttaka*, ou método da *pulverização*, adotado pelos antigos astrônomos hindus ([122], páginas 114 e 115).

**Problema resolvido 11.1.** Encontre as soluções de $19x + 4y = 3$, para $x, y \in \mathbb{Z}$.

*Solução.* Como $\text{mdc}(19, 4) = 1$ e $1 \mid 3$ então a equação dada tem solução. Como $19 = 4 \cdot 4 + 3$ temos $(4 \cdot 4 + 3)x + 4y = 3 \iff 4(4x + y) + 3x = 3$. Pondo $z = 4x + y$ obtemos a primeira redução $4z + 3x = 3$. Essa última pode ser escrita na forma $z + 3(z + x) = 3 \iff z + 3w = 3$ com $w = z + x$. Tomando $w = t$ como parâmetro vem $z = 3 - 3t \Rightarrow x = w - z = 4t - 3 \Rightarrow y = z - 4x = 15 - 19t$. Portanto as soluções são $(x, y) = (4t - 3, 15 - 19t)$ para todo $t \in \mathbb{Z}$. □

Confira a seguinte variação do método da pulverização, utilizada por Leonard P. Euler em seu livro *Algebra*, de 1770. Para resolver $5x - 17y = 3$ observamos que $17 = 3 \cdot 5 + 2$ e escrevemos

$$x = \frac{17y + 3}{5} = \frac{3 \cdot 5y + 2y + 3}{5} = 3y + \frac{2y + 3}{5}.$$

O número $(2y + 3)/5$ deve ser um inteiro. Chamando-o de $z$ temos

$$\frac{2y + 3}{5} = z \iff 2y + 3 = 5z \iff 2y - 5z = -3.$$

Repetindo o processo para essa última equação temos

$$y = \frac{5z - 3}{2} = 2z - 1 + \frac{z - 1}{2},$$

e $(z - 1)/2$ deve ser um inteiro, digamos $(z - 1)/2 = w$. Então $z - 1 = 2w$. Tomando $w = t$ como parâmetro, vem $z = 2t + 1 \Rightarrow$

$$y = \frac{5z - 3}{2} = \frac{5(2t + 1) - 3}{2} = 5t + 1$$

e

$$x = \frac{17y + 3}{5} = \frac{17(5t + 1) + 3}{5} = 17t + 4.$$

Portanto as soluções são $(x, y) = (17t + 4, 5t + 1)$ para todo $t \in \mathbb{Z}$.

Terminamos esta seção apresentando uma observação que permite resolver rapidamente a equação $52x + 3y = 12$. Como $3 \mid 12 - 3y$ então $3 \mid 52x \Rightarrow 3 \mid x$. Escrevemos $x = 3x_1$. A equação dada se reduz a $52x_1 + y = 4$. Tomando $x_1 = t$ como parâmetro vem $x = 3t$ e $y = 4 - 52t$. Portanto as soluções são $(x, y) = (3t, 4 - 52t)$ para todo $t \in \mathbb{Z}$.

## 11.4 Uma fórmula para as soluções

É dada pelo seguinte

**Teorema 11.2.** *Sejam $a$, $b$ e $c$ números inteiros com $a \neq 0$ e $b \neq 0$. A equação diofantina linear*

$$ax + by = c, \quad \text{com } x, y \in \mathbb{Z},$$

*tem solução se e somente se $d = \text{mdc}(a, b)$ é divisor de $c$. Nesse caso, se $(x_0, y_0)$ é uma solução, então as soluções são dadas por $(x, y) = (x_0 + \frac{b}{d}t, y_0 - \frac{a}{d}t)$ para todo $t \in \mathbb{Z}$.*

*Demonstração.* Se $x_0, y_0 \in \mathbb{Z}$ são tais que $ax_0 + by_0 = c$ então $d \mid a$ e $d \mid b$ implicam $d \mid c$. Reciprocamente, se $d \mid c$, seja $c = c_1 d$. Sabemos que existem inteiros $r$ e $s$ tais que $ra + sb = d$. Logo $a(c_1 r) + b(c_1 s) = c_1 d = c$, e $(x_0, y_0) = (c_1 r, c_1 s)$ é uma solução.

Para demonstrar a segunda parte do Teorema, observamos primeiro que se $(x_0, y_0)$ é uma solução, então $(x, y) = (x_0 + \frac{b}{d}t, y_0 - \frac{a}{d}t)$ é uma solução para todo $t \in \mathbb{Z}$. De fato,

$$a\left[x_0 + \frac{b}{d}t\right] + b\left[y_0 - \frac{a}{d}t\right] = ax_0 + by_0 = c.$$

Vamos mostrar que toda solução é dessa forma. Seja $(x_1, y_1)$ uma solução qualquer. Então $ax_0 + by_0 = ax_1 + by_1$ o que implica $b(y_0 - y_1) = a(x_1 - x_0)$. Ponhamos $a = a_1 d$ e $b = b_1 d$. Então $a_1$ e $b_1$ são relativamente primos e $b_1(y_0 - y_1) = a_1(x_1 - x_0)$. Portanto $b_1 \mid x_1 - x_0$, e existe $t \in \mathbb{Z}$ tal que $x_1 - x_0 = tb_1$. Substituindo isso em $b_1(y_0 - y_1) = a_1(x_1 - x_0)$ vem $y_0 - y_1 = ta_1$. Portanto $x_1 = x_0 + \frac{b}{d}t$ e $y_1 = y_0 - \frac{a}{d}t$. Chegamos assim à forma desejada. □

**Problema resolvido 11.3.** Encontre as soluções de $78x + 105y = 51$, para $x, y \in \mathbb{Z}$, usando a fórmula do Teorema 11.2.

*Solução.* Primeiro necessitamos calcular $\text{mdc}(78, 105)$. Usamos o algoritmo euclidiano, o que nos permite também calcular uma solução particular. Temos

$$105 = 1 \cdot 78 + 27, \;\; 78 = 2 \cdot 27 + 24, \;\; 27 = 1 \cdot 24 + 3, \;\; 24 = 8 \cdot 3 + 0,$$

o que nos leva a $\text{mdc}(78, 105) = 3$. Como $3 \mid 51$, vemos que a equação dada tem infinitas soluções. Para obter inteiros $r$ e $s$ tais que $78r + 105s = 3$ fazemos $3 = 27 - 24 = 27 - (78 - 2 \cdot 27) = 3 \cdot 27 - 78 = 3(105 - 78) - 78 = 78(-4) + 3 \cdot 105$. Portanto

$$78(-4 \cdot 17) + 105(3 \cdot 17) = 3 \cdot 17 \Rightarrow 78(-68) + 105(51) = 51.$$

Dessa forma $(x_0, y_0) = (-68, 51)$ é uma solução, e a solução geral dada pela fórmula do Teorema 11.2 é

$$(x, y) = \left(-68 + \frac{105}{3}t, 51 - \frac{78}{3}t\right) = (-68 + 35t, 51 - 26t), \; t \in \mathbb{Z}.$$

□

**Observação 11.4.** No exemplo acima, depois de calcular $\text{mdc}(78, 105) = 3$ e constatar que $3 \mid 51$, podemos simplificar a equação por 3, e resolver a equação equivalente $26x + 35y = 17$.

## 11.5 Problemas

**Problema 11.5.1.** Analise a equação 11.1 quando $c = 0$.

**Problema 11.5.2.** Mostre que a equação diofantina linear $3x - 29y = 1$, com $x, y \in \mathbb{Z}$, tem infinitas soluções. Encontre-as utilizando o método da pulverização. Resolva também essa mesma equação com a fórmula apresentada no Teorema 11.2. Compare os dois métodos.

**Problema 11.5.3.** Este problema faz parte da coleção de enigmas publicados por Claude G. Bachet em 1612. "41 pessoas tomam parte de uma refeição. A conta é de 41 *sous*. Cada homem paga 4 *sous*, cada mulher, 3 e cada criança $\frac{1}{3}$ de *sous*. Quantos são os homens, e as mulheres, e as crianças?".

**Problema 11.5.4.** Dentre os problemas compilados por Alcuin de York, na Idade Média, consta o seguinte. "Se 100 *bushels* de grãos são distribuídos entre 100 pessoas de modo que cada homem receba três *bushels*, cada mulher, dois, e cada criança, metade de um *bushel*, quantos são os homens, e as mulheres, e as crianças?"

**Problema 11.5.5.** Um problema extraído da obra *Algebra*, de Leonard P. Euler: "Um homem comprou cavalos e vacas gastando um total de $ 1770. Cada cavalo custou $ 31 e cada vaca, $ 21. Quantos cavalos e quantas vacas foram comprados?"

**Problema 11.5.6.** Encontre o menor inteiro positivo que tem restos 3 e 7 quando dividido, respectivamente, por 5 e 11.

**Problema 11.5.7.** Um comerciante tem 500 litros de um certo produto que devem ser distribuídos em recipientes de 3 e 5 litros. Quantos recipientes de cada tipo devem ser adquiridos de modo a minimizar seu custo?

**Problema 11.5.8.** Exprimir o número 100 como soma de dois inteiros positivos de modo que o primeiro seja divisível por 7 e o segundo por 11.

**Problema 11.5.9.** Dispomos de duas ampulhetas, uma mede 6 minutos, outra mede 11. Como medir 13 minutos?

**Problema 11.5.10.** Confira os detalhes da seguinte versão geral do método da pulverização. Consideremos a equação diofantina linear $a_1x_2 + a_2x_1 = c$, dados $a_1, a_2, c \in \mathbb{Z}$, $a_1 \neq 0$, $a_2 \neq 0$, tais que $d = \text{mdc}(a_1, a_2) \mid c$. Simplificando a equação por $d$ podemos supor $d = 1$. Aplicando o algoritmo euclidiano a $a_1$ e $a_2$ temos

$$\begin{array}{rcll} a_1 & = & q_1a_2 + a_3 & 0 < a_3 < |a_2| \\ a_2 & = & q_2a_3 + a_4 & 0 < a_4 < a_3 \\ a_3 & = & q_3a_4 + a_5 & 0 < a_5 < a_4 \\ \vdots & & & \\ a_{n-3} & = & q_{n-3}a_{n-2} + a_{n-1} & 0 < a_{n-1} < a_{n-2} \\ a_{n-2} & = & q_{n-2}a_{n-1} + a_n & \end{array}$$

em que $a_n = 1$ é o $\text{mdc}(a_1, a_2)$.

Utilizamos as seguintes variáveis auxiliares:

$$\begin{array}{rcl} x_3 & = & q_1x_2 + x_1 \\ x_4 & = & q_2x_3 + x_2 \\ x_5 & = & q_3x_4 + x_3 \\ \vdots & & \\ x_n & = & q_{n-2}x_{n-1} + x_{n-2} \end{array}$$

Introduzindo $a_1 = q_1a_2 + a_3$ em $a_1x_2 + a_2x_1 = c$ vem $a_2(q_1x_2 + x_1) + a_3x_2 = c$, ou $a_2x_3 + a_3x_2 = c$. E assim sucessivamente, após a última substituição, vem $a_{n-1}x_n + a_nx_{n-1} = c$, ou $a_{n-1}x_n + x_{n-1} = c$. Tomando $x_n = t$ como parâmetro obtemos $x_{n-1}$ em função de $t$, depois $x_{n-2}$, e sucessivamente, no final das substituições, obtemos $x_2$ e $x_1$ em função de $t$.

## 11.6 Temas para investigação

**Tema 11.6.1.** Investigue métodos de resolução de equações diofantinas lineares com $n$ variáveis da forma

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b, \quad \text{com } x_i \in \mathbb{Z}, \tag{11.3}$$

em que $a_i \neq 0$ são inteiros para todo $i$. Encontre condições necessárias e suficientes para que exista solução.

**Tema 11.6.2.** Num tabuleiro infinito de xadrez, o cavalo, partindo de uma determinada casa, pode atingir quais outras casas?

**Tema 11.6.3.** Um sapo sobe uma escada com degraus numerados a partir de 1. O sapo só dá saltos de 5 ou 7 degraus de cada vez. Por exemplo, partindo do chão, o sapo pode chegar ao 17º degrau dando dois saltos de 5 e um de 7. Poderá o sapo chegar ao 23º degrau? Quais são os degraus que o sapo pode atingir?

Estude a seguinte generalização. Sejam $a$ e $b$ números inteiros positivos. Encontre a estrutura do conjunto $S = \{ax + by \mid x, y \in \mathbb{Z}, x \geq 0, y \geq 0\}$.

**Tema 11.6.4.** O sapo do tema anterior agora dá saltos de 5 ou 7 ou 11 degraus de cada vez. Estude a estrutura do conjunto $S = \{5x + 7y + 11z \mid x, y, z \in \mathbb{Z}, x \geq 0, y \geq 0, z \geq 0\}$.

# Capítulo 12

# Aplicativos computacionais para TN

## 12.1 Introdução

Os aplicativos computacionais algébricos constituem atualmente o principal recurso disponibilizado pela Ciência da Computação para aprendizagem e investigação em Teoria dos Números (TN). Sua capacidade em realizar cálculos numéricos e algébricos é significativa, e proporcionam um novo patamar de possibilidades para a Matemática, assim como para outras áreas do conhecimento.

Neste Capítulo colocamos nossa atenção em aplicativos algébricos de domínio público, mas fazemos alguns comentários sobre os comerciais.

Alertamos os estudantes de Matemática para a importância do aprendizado de algoritmos, assim como de linguagens de programação. Em particular, aproveitamos a oportunidade para fazer uma chamada de atenção para a IA, que traz grandes possibilidades.

## 12.2 Decrição sumária de alguns aplicativos

Já vai longe o tempo em que matemáticos contratavam indivíduos com capacidade excepcional em cálculos aritméticos para ajudá-los em suas pesquisas. Alguns matemáticos também se dedicaram à invenção e construção de máquinas mecânicas de calcular. Um exemplo foi Blaise Pascal, que construiu muitos exemplares da máquina Pascalina, capaz de implementar adição e subtração. Podia ainda fazer multiplicação e divisão através de somas e subtrações sucessivas. Gottfried W. Leibniz também se dedicou a esse mister, e sua proposta se aproximou das máquinas mecânicas que posteriormente povoaram os escritórios.

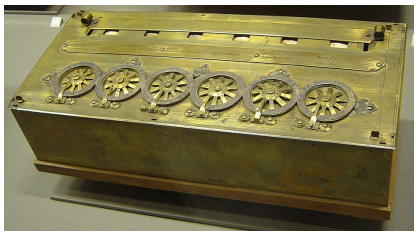


Figura 12.1. Blaise Pascal (1623-1662) foi um matemático, físico, inventor, filósofo e teólogo francês. Considerado um prodígio, tem seu nome ligado a várias áreas, como o triângulo de Pascal em Teoria dos Números e o Princípio de Pascal em Teoria dos Fluidos. Para ajudar seu pai em seu trabalho de contador, inventou uma calculadora mecânica, a Pascalina. Ao lado, foto de exemplar depositado no Museu de Artes e Ofícios de Paris (mais detalhes na página 262).

O reinado das calculadoras mecânicas se encerrou com o aparecimento da microeletrônica e das calculadoras digitais. Surgiram no início da década de 1960, e hoje existem muitos modelos para atender às mais variadas finalidades e com os mais diferentes preços.

Ainda no início da década de 1960 o progresso na engenharia de software permitiu o surgimento dos primeiros sistemas de computação simbólica, atrelados às pesquisas em Inteligência Artificial. Destacaram-se o Formac, o Lisp e o Alpac. No fim dessa mesma década veio a segunda geração, e tornaram-se populares o Reduce, o Macsyma e o MuMath. A partir da década de 1980 os sistemas genéricos Maple, Mathematica e MathLab são líderes no segmento comercial. Como softwares gratuitos se destacam o Maxima e o SageMath. Existem também sistemas especializados, que atendem a segmentos específicos. Consulte [128] no verbete *Sistema algébrico computacional*.

Os sistemas de computação simbólica representam um avanço considerável em relação aos dispositivos que os antecederam. São capazes de: precisão aritmética arbitrária; facilidades gráficas, incluindo gráficos de funções; manipulação simbólica, como lidar com expressões algébricas, resolver equações, derivar e integrar funções, etc.; executar programação de alto nível.

Neste texto destacamos os sistemas Maxima e SageMath por terem distribuição gratuita.

**Maxima** é um software matemático e um aplicativo computacional algébrico, básico mas muito bom para estudantes e profissionais de Matemática e outras ciências. Foi construído sobre uma versão de 1982 do Macsyma e lançado também em 1982. É desenvolvido pelo Grupo Macsyma e colaboradores voluntários. É um software livre disponibilizado sob os termos da GNU General Public License (GPL). A interface gráfica mais usada é o wxMaxima. Para mais detalhes consulte a Wikipedia [128] no verbete *Máxima (software)*.

**SageMath** é um software matemático e um aplicativo computacional algébrico bastante completo, lançado em 2005 com distribuição gratuita sob os termos da GNU General Public License (GPL). Seu principal desenvolvedor é William A. Stein, um especialista em aritmética computacional. Os recursos do SageMath abrangem álgebra, combinatória, teoria dos grafos, teoria dos grupos, variedades diferenciáveis, análise numérica, teoria dos números, cálculo diferencial e integral e estatística. Para mais detalhes consulte a Wikipedia [128] no verbete *SageMath*.

**Maple** Sistema comercial, desenvolvido desde 1988 pela Maplesoft, uma companhia canadense. Lida com praticamente todas as áreas científicas, e disponibiliza biblioteca de aplicativos para as mais diversas finalidades com programação de alto nível. A Maplesoft comercializa o Maple em versão profissional e estudantil. Para mais detalhes consulte a Wikipedia [128] no verbete *Maple*.

**Wolfram Mathematica**, ou, simplesmente, *Mathematica*, sistema comercial, considerado o mais completo. Foi criado por Stephen Wolfram, e desenvolvido pela empresa estadunidense Wolfram Research. O primeiro lançamento foi em 1988, e é comercializado em várias versões. Opera com as ciências exatas e biológicas, engenharias, economia, música, artes e jogos. Tem programas especiais para ensino da Matemática. Para mais detalhes consulte a Wikipedia [128] no verbete *Mathematica*.

## 12.3 Um pouco de TN no Maxima

Alguns comandos iniciais, separados em dois grupos.

### 12.3.1 Exemplos em Aritmética

Começamos com algumas observações gerais. Uma linha de comando deve terminar com ; (ponto e vírgula). O comando é executado com as teclas Ctrl+Enter. A resposta é transcrita

na linha logo abaixo. Para fazer comentário coloque-o entre /* e */ o interpretador do Maxima ignora o que está escrito ali. Exemplo:

```
(%i1)  3*7;  /*  use a tecla * para indicar multiplicação  */
(%o1)  21
```

Os símbolos aritméticos são:

| | | | |
|---|---|---|---|
| + | adição | − | subtração |
| ⋆ | multiplicação | / | divisão e fração |
| ∧ | potenciação | sqrt(n) | raiz quadrada de n |
| ! | fatorial | nthroot(x,m) | raiz $m$-ésima de $x$ (se for exata) |

Exemplos (vários comandos podem ser escritos numa mesma linha):

```
(%i7)  8 + 2;  8 − 2;  8 * 2;  8/2;  5/2;  8^2;  8!;
(%o1)  10
(%o2)  6
(%o3)  16
(%o4)  4
(%o5)  5/2
(%o6)  64
(%o7)  40320
```

Outros exemplos com frações. Tipicamente, números não inteiros são expressos com 16 casas, contando antes e depois da vírgula (que no Maxima é expressa por ponto).

```
(%i6)  5.0/2;  30/21;  1/3;  1.0/3;  float(1/3);  1/3, numer;
(%o1)  2.5
(%o2)  10/7
(%o3)  1/3
(%o4)  0.333333333333333
(%o5)  0.333333333333333
(%o6)  0.333333333333333
```

Exemplos com raízes quadradas.

```
(%i5)  sqrt(4);  sqrt(5);  sqrt(5.0);  sqrt(8);  float(sqrt(5));
(%o1)  2
(%o2)  sqrt(5)
(%o3)  2.23606797749979
(%o4)  2^(3/2)
(%o5)  2.23606797749979
```

Exemplos com raízes $n$-ésimas.

```
(%i5)  nthroot(8, 3);  nthroot(9, 3);  8^(1/3);  9^(1/3);  9.0^(1/3);
(%o1)  2
(%o2)  nthroot: 9 is not a "third" power
(%o3)  2
(%o4)  9^(1/3)
(%o5)  2.080083823051904
```

Em expressões aritméticas, a ordem hierárquica das operações no Maxima é: 1. parênteses e, em seguida, fatorial e depois expoentes; 2. multiplicação e divisão, na ordem em que aparecem, da esquerda para a direita; 3. adição e subtração, na ordem em que aparecem, da esquerda para a direita. Na dúvida, ou para seguir outro caminho, use parêntesis. Exemplos:

```
(%i8)  8-5+3*2;  8/2*4;  8/(2*4);  16/8/2;  16/(8/2);  2+2^3;  2^4/2;  3^2!;
(%o1)  9
(%o2)  16
(%o3)  1
(%o4)  1
(%o5)  4
(%o6)  10
(%o7)  8
(%o8)  9
```

Assim $8-5+3*2$ é interpretado como $8-5+(3*2)=8-5+6$, em seguida $(8-5)+6=3+6=9$. Para seguir um caminho diferente é preciso usar parêntesis.

Uma dica final para esta Subseção. As expressões para o número de Arquimedes $\pi$, o número de Neper $e$ e a unidade imaginária $i$ são, respectivamente, %pi, %e %i. Exemplos:

```
(%i7)  %pi; %i*%i; float(%pi); float(%e); compare(%pi^%e,%e^%pi); fpprec:30; bfloat(%pi);
(%o1)  π
(%o2)  -1
(%o3)  3.141592653589793
(%o4)  2.718281828459045
(%o5)  <
(%o6)  30
(%o7)  3.14159265358979323846264338328b0
```

Para obter o valor numérico de $\pi$ com mais casas é necessário primeiro assinalar o valor desejado à variável fpprec e depois usar o comando bfloat( ).

### 12.3.2 Exemplos em TN

Começamos com uma pequena lista de comandos relacionados com TN:

**binomial(a,b)** retorna o valor do número binomial $\binom{a}{b}$.

**ceiling(x)** ($x$ real) retorna o menor inteiro $\geq x$.

**divide(a,b)** retorna o quociente e o resto da divisão euclidiana de $a$ por $b \neq 0$.

**divisors(n)** retorna o conjunto dos divisores positivos de $n$.

**divsum(n)** retorna a soma dos divisores positivos de $n$, incluindo 1 e $n$.

**factor(n)** retorna a decomposição canônica de $n$.

**fib(n)** retorna o termo de ordem $n+1$ da sequência de Fibonacci, começando com fib(0)=0 e fib(1)=1.

**floor(x)** ($x$ real) retorna o maior inteiro $\leq x$.

**gcd(a,b)** retorna mdc$(a,b)$. Para mais de dois números, use propriedades.

**ifactors(n)** retorna a decomposição canônica de $n$ na forma de listas [primo,expoente].

**integer_partitions(n)** retorna as partições de $n$ como soma de inteiros positivos na forma de conjunto de listas.

**integerp(expr)** retorna true se expr corresponde a um inteiro, e false do contrário.

**inrt(x,n)** com $x$ real e n inteiro positivo. Retorna $\left[\sqrt[n]{|x|}\right]$ (parte inteira).

**isqrt(x)** o mesmo que inrt(x,2).

**lcm(a,b,...)** retorna mmc$(a, b, ...)$.

**mod(a,m)** retorna $a$ módulo $m$, isto é, o resto da divisão euclidiana de $a$ por $m$.

**next_prime(n)** retorna o menor primo maior do que $n$.

**num_partitions(n)** retorna o número de partições de $n$ inteiro não negativo.

**num_partitions(n,list)** retorna a lista dos números de partições de 1, 2, 3, ..., $n$.

**power_mod(a,n,m)** retorna $a^n$ módulo $m$, isto é, o resto da divisão euclidiana de $a^n$ por $m$.

**prev_prime(n)** retorna o maior primo menor do que $n$.

**primep(n)** comando probabilístico. Se retorna false então $n$ é composto. Se $n < 10^{16}$ e se retorna true, então $n$ é primo. Se $n \geq 10^6$ e se retorna true, $n$ é provavelmente primo.

**round(x)** ($x$ real) retorna a parte inteira de $x$.

**totient(n)** retorna o número de inteiros positivos menores ou iguais a n e relativamente primos com $n$. Essa é a função $\varphi$ de Euler.

Exemplos:

```
(%i6)  divisors(6); divsum(6); factor(24); ifactors(24);gcd(-24,78); lcm(5,7,24,78);
(%o1)  {1, 2, 3, 6}
(%o2)  12
(%o3)  2^3 3
(%o4)  [[2,3],[3,1]]
(%o5)  6
(%o6)  10920
```

Mais exemplos:

```
(%i5)  binomial(14,5); inrt(9,3); mod(5,2); power_mod(12,7,5); totient(5);
(%o1)  2002
(%o2)  2
(%o3)  1
(%o4)  3
(%o5)  4
```

Exemplos de primaridade:

```
(%i4)  primep(34567); prev_prime(34567); next_prime(34567); next_prime(1000000);
(%o1)  false
(%o2)  34549
(%o3)  34583
(%o4)  1000003
```

Os 11 primeiros termos da sequência de Fibonacci:

```
(%i1)  map(fib, [0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10]);
(%o1)  [0,1,1,2,3,5,8,13,21,34,55]
```

Uma orientação completa sobre os comandos do Maxima pode ser obtida em [75] ou em [2]. Consulte também [5].

## 12.4 Problemas

**Problema 12.4.1.** Consultando o Problema 4.4.9 defina no Maxima números pentagonais $P(n)$, e calcule os dez primeiros.

**Problema 12.4.2.** O comando primep(34567); retornou false. Obtenha a decomposição canônica de 34567.

**Problema 12.4.3.** Use o Maxima para verificar que 503 e 809 são primos, o que foi pedido no Problema 4.10.7. Igualmente para 38567 (Problema 5.5.2).

**Problema 12.4.4.** Use o Maxima para verificar que 458 941 é múltiplo de 7, conforme pedido no Problema 4.10.24.

**Problema 12.4.5.** Use o Maxima para encontrar a decomposição canônica, assim como os divisores, de: 120; 375; 539; 2015; 1 455 521; conforme solicitado nos Problemas 5.7.5 e 5.7.6.

**Problema 12.4.6.** Use o Maxima para confirmar as afirmações do Problema 5.9.6.

**Problema 12.4.7.** Use o Maxima para resolver os Problemas 5.11.14 e 5.11.15.

**Problema 12.4.8.** 144 e 1444 são quadrados perfeitos. Você quer fazer uma conjectura? E quanto a 49, 4489, 444889, 44448889, ... ?

**Problema 12.4.9.** No Século XV Luca Pacioli afirmou que $1 + 2 + 2^2 + \cdots + 2^{26}$ seria primo. Verifique que a afirmação não é verdadeira.



Figura 12.2. Luca Bartolomeu de Pacioli foi um Frei Franciscano, matemático e escritor italiano do Século XV. Desenvolveu a Aritmética, e é considerado o pai dos contadores. Traduziu para o latim Os Elementos, de Euclides. Sua obra mais famosa é *Divina proportione*, em que trata da proporção artística e da razão áurea. Ao lado, foto de pintura de Pacioli feita por Jacopo de Barbari, depositada no Museu de Capodimonti (mais detalhes na página 262).

## 12.5 Pequenos programas em TN

Para listar os números de 1 a 20:

```
(%i1)   makelist(n,n,1,20);
(%o1)   [1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20]
```

Se quiser somar os números de 1 a 100 (sem usar fórmula), pode ser assim:

```
(%i1)  sum(n,n,1,100);
(%o1)  5050
```

Explicação: em (n,n,1,100) o primeiro n estabelece o nome de uma variável, e n,1,100 diz que essa variável deve percorrer os números naturais de 1 a 100. O comando makelist pede para listá-los, e o comando sum pede para somá-los.

Um pouco mais sofisticado para executar o mesmo procedimento é seguinte bloco de comandos. Dentro do bloco, os comandos são separados por vírgula.

```
(%i1)  block([S], S:0, for i:1 while i<=100 do S:S+i, return(S));
(%o1)  5050
```

Explicação: o comando [S] estabelece o nome de uma variável para a soma. S:0 diz que o valor inicial da variável é zero. for i:1 chama a variável auxiliar i e estabelece que seu valor inicial é 1. while i<=100 do S:S+i diz que i deve percorrer os números inteiros de 1 a 100, e, a cada valor, soma S com i. return(S) pede para dar como resposta o valor de S.

Para obter uma lista dos números triangulares, primeiro definimos a função $T(n) = \frac{n(n+1)}{2}$. Depois pedimos a lista. Seguem os 11 primeiros números triangulares, a partir de $T(0)$.

```
(%i2)  T(n):=n*(n+1)/2; makelist(T(n),n,0,10);
(%o1)  T(n) = n(n+1)/2
(%o2)  [0,1,3,6,10,15,21,28,36,45,55]
```

Uma alternativa:

```
(%i2)  T(n):=n*(n+1)/2; map(T, [0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10]);
(%o1)  T(n) = n(n+1)/2
(%o2)  [0,1,3,6,10,15,21,28,36,45,55]
```

Outro jeito:

```
(%i1)  T(n):=n*(n+1)/2; for n:0 thru 10 do print("T(",n,")=",T(n));
(%o1)  T(n) = n(n+1)/2
       T(0)=0
       T(1)=1
       T(2)=3
       T(3)=6
       T(4)=10
       T(5)=15
       T(6)=21
       T(7)=28
       T(8)=36
       T(9)=45
       T(10)=55
```

Vejamos como produzir os dados da tabela disponibilizada no Tema 6.7.3. Podemos calcular a decomposição canônica de $2^n + 1$ para $n = 1, 2, 3, ...$

```
(%i5)  factor(2^1+1); factor(2^2+1); factor(2^3+1); factor(2^4+1); factor(2^5+1);
(%o1)  3
(%o2)  5
(%o3)  3^2
(%o4)  17
(%o5)  3 11
```

Prosseguimos calculando mais cinco termos, e assim até o desejado. Mais confortável e informativo é o seguinte programa:

```
(%i1)  h(n):=2^n+1; for n:1 thru 18 do display(n,h(n),factor(h(n)));
```
$h(n) = 2^n + 1$
$n = 1$
$h(1) = 3$
factor(3)=3
$\vdots$
$n = 18$
$h(18) = 262145$
factor(262145)=5 13 37 109
done

Usando listas fica melhor ainda:

```
(%i1)  h(n):=2^n+1; L(n):=list(n,h(n),factor(h(n))); for n:1 thru 18 do display(L(n));
```
$h(n) = 2^n + 1$
L(n):=list(n,h(n),factor(h(n)))
L(1)=list(1,3,3)
L(2)=list(2,5,5)
L(3)=list(3,9,$3^2$)
$\vdots$
L(18)=list(18,262145,5 13 37 109)
done

Encerramos esta seção resolvendo o Tema 4.14.10, em que foi pedido escrever cada um dos 50 primeiros números naturais como soma de três números triangulares (não necessariamente diferentes). Para isso compilamos (para não usar muito espaço do texto limitamos a $n = 10$):

```
(%i1)  T(n):=n*(n+1)/2; for n:0 thru 10 do for i:0 thru 10 do for j:0 thru 10 do
       for k:0 thru 10 do if n=T(i)+T(j)+T(k) and i<=j and j<=k then
       print(n,"=","T(",i,")+T(",j,")+T(",k,")");
```
(%o1) $T(n) = \frac{n(n+1)}{2}$
0=T(0)+T(0)+T(0)
1=T(0)+T(0)+T(1)
2=T(0)+T(1)+T(1)
3=T(0)+T(0)+T(2)
3=T(1)+T(1)+T(1)
4=T(0)+T(1)+T(2)
5=T(1)+T(1)+T(2)
6=T(0)+T(0)+T(3)
6=T(0)+T(2)+T(2)
7=T(0)+T(1)+T(3)
7=T(1)+T(2)+T(2)
8=T(1)+T(1)+T(3)
9=T(0)+T(2)+T(3)
9=T(2)+T(2)+T(2)
10=T(0)+T(0)+T(4)
10=T(1)+T(2)+T(3)

Para obter explicações mais completas sobre programação no Maxima consulte [5] a partir da página 165, assim como [72].

## 12.6 Problemas

**Problema 12.6.1.** Use o Maxima para calcular o produto $1 \cdot 3 \cdot 5 \cdot 7 \cdot \ldots \cdot 57$ dos ímpares de 1 a 57 e determinar seu dígito das unidades. O que ocorre se for até 2007, como no Problema 4.8.18?

**Problema 12.6.2.** Faça um programa para resolver a segunda parte do Problema 4.10.11. Isto é, encontre pelo menos um número primo da forma $n = (11\ldots1)_{dez}$ maior do que 11 sem precisar testar a primaridade um por um. Aproveite ainda para rever suas investigações no Tema 5.16.5.

**Problema 12.6.3.** Faça um programa para ajudá-lo com o Tema 5.16.8. Para expoentes muito grandes é necessário um programa especial.

**Problema 12.6.4.** Faça uma tabela das rep-unidades $n = (11\ldots1)_{dez}$ e sua respectiva decomposição canônica. Faça conjecturas e tente demonstrá-las. Por exemplo, quais rep-unidades são múltiplas de 101?

**Problema 12.6.5.** Faça uma tabela dos números $2^n + (-1)^{n+1}$ e sua respectiva decomposição canônica. Observe regularidades, faça conjecturas e tente demonstrá-las.

**Problema 12.6.6.** Sugestões de expressões adicionais para que você possa fazer investigações: **a)** $3^{2n} - 1$; **b)** $2^{3n} - 1$; **c)** $3^{2n+} + 2^{n+2}$; **d)** $3n^5 + 5n^3 + 7n$; **e)** $n^2(n^2 - 1)(n^2 - 4)$.

**Problema 12.6.7.** Charles de Bovelles, autor do primeiro livro científico impresso na França, conjecturou que para todo número natural $n$, $6n - 1$ ou $6n + 1$ é primo. Faça um programa para descobrir o menor $n$ para o qual falha essa conjectura.

**Problema 12.6.8.** Conjectura-se que existem infinitos primos $p$ para os quais $p + 50$ também é primo. Encontre 20 exemplos fazendo um programa no Maxima.

**Problema 12.6.9.** Use um programa do Maxima para verificar a seguinte afirmação do Problema 7.7.12: o produto dos primos ímpares $< 100$ é

$$P = 115278398197275921237655107366587803 5.$$

**Problema 12.6.10.** O matemático inglês Godfrey H. Hardy conta uma história sobre seu amigo também matemático Srinivasa Ramanujan. Hardy, dirigindo-se ao hospital onde seu amigo se recuperava de uma doença, tomou um taxi, e notou que o número da licença do mesmo era 1729. Chegando ao hospital, observou a Ramanujan que esse número parecia muito desinteressante. — Não, refletiu ele, trata-se de um número muito interessante, pois é o menor número que pode ser escrito como soma de dois cubos de duas maneiras diferentes. Como o Maxima pode ser usado para verificar a afirmação de Ramanujan?

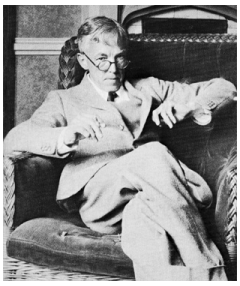


Figura 12.3. Godfrey H. Hardy (1877-1947) matemático e professor nas Universidades de Cambridge e Oxford. Especialista em Teoria dos Números e Análise Matemática, contribuiu também em Biologia. Cultivou diversas parcerias com outros matemáticos, sendo a mais conhecida com S. Ramanujan, matemático hindu, a quem ele acolheu para trabalhar na Inglaterra. Ao lado, foto de Hardy (mais detalhes na página 262).

## 12.7 Aplicativos de Inteligência Artificial

Esses aplicativos também podem ser usados para aprendizagem e investigação em TN. Embora tenham sido disponibilizados recentemente para o público, muitas experiências estão sendo desenvolvidas. Não fazemos aqui um exame aprofundado dessa ferramenta. Procuramos apenas incentivar o estudante a empreender sua própria exploração.

Perguntamos à IA do Google o seguinte: $n^2+8$ é primo para $n$ múltiplo de 3 e ímpar?

Tivemos interesse nessa pergunta no momento em que estávamos redigindo o Tema de Investigação 5.16.11. Foi comentado que $n^2+8$ pode ser primo para $n$ múltiplo de 3 e ímpar. Em particular, isso é válido para $n = 3$, 9, 15 e 21, como foi observado no Problema Resolvido 5.2. Ali também foi verificado que $n^2+8$ não é primo se $n$ não é múltiplo de 3. Tampouco se $n$ for par, pois isso implica que $n^2+8$ é par $> 2$.

A intenção desse problema é que o estudante perceba que não é tão fácil encontrar fórmulas para números primos (muito menos para todos os primos). O que é esperado é que tais fórmulas possam fornecer primos para alguns valores, mas logo se acha contra-exemplo. No caso, para $n = 27$, se tem $n^2+8 = 737 = 11 \cdot 67$ , e para $n = 39$, $n^2+8 = 1529 = 11 \cdot 139$, que não são primos.

Procurando mais alguma informação, lembrei-me de perguntar ao Google, e obtive a seguinte resposta:

*Resposta da IA em abril de 2025 (o destaque em negrito foi dela)*:

"**Não**. Para $n$ ser um múltiplo de 3 e ímpar, $n = 3k$, onde $k$ é um inteiro ímpar. Assim, $n^2 = (3k)^2 = 9k^2$. Logo, $n^2+8 = 9k^2+8$. Para $k = 1$, $n^2+8 = 9+8 = 17$, que é primo. Para $k = 3$, $n^2+8 = 81+8 = 89$, que é primo. Para $k = 5$, $n^2+8 = 225+8 = 233$, que é primo. No entanto, para $k = 7$, $n^2+8 = 441+8 = 449$, que é primo. Portanto, não é possível determinar se $n^2+8$ é sempre primo quando $n$ é um múltiplo ímpar de 3."

Vemos que a IA, naquela data, ainda precisava de calibração. Além de algumas discrepâncias semânticas, a resposta está apenas parcialmente correta. A IA percorreu a mesma linha de raciocínio quando nos deparamos com esse tipo de questão: procuramos alguns exemplos. Mas a IA não foi suficientemente persistente para encontrar um contra-exemplo (seria no próximo valor ímpar de $k$). Mesmo assim, deu um **não** como resposta, de alguma forma concluiu corretamente.

Um mês depois repetimos a pergunta, e desta vez obtivemos o seguinte:

*Segunda resposta da IA em junho de 2025 (o destaque em negrito foi dela, o destaque da caixa é nosso)*:

"**Não**. $n^2+8$ não é necessariamente primo quando $n$ é um múltiplo de 3 e ímpar.

Explicação:
Se $n$ é múltiplo de 3, então $n$ pode ser escrito como $3k$, onde $k$ é um inteiro. Se $n$ é também ímpar, então $k$ também deve ser ímpar.
Se $n = 3$, então $n^2 + 8 = 3^2 + 8 = 9 + 8 = 17$, que é primo.
Se $n = 9$, então $n^2 + 8 = 9^2 + 8 = 81 + 8 = 89$, que é primo.
Se $n = 15$, então $n^2 + 8 = 15^2 + 8 = 225 + 8 = 233$, que é primo.
Se $n = 21$, então $n^2 + 8 = 21^2 + 8 = 441 + 8 = 449$, que é primo.
Se $n = 27$, então $n^2 + 8 = 27^2 + 8 = 729 + 8 = 737$, que é composto $\boxed{(737 = 19 * 37)}$.
Se n $= 33$, então $n^2 + 8 = 33^2 + 8 = 1089 + 8 = 1097$, que é primo.

Portanto, não é sempre que $n^2 + 8$ é primo quando $n$ é múltiplo de 3 e ímpar.

Conclusão:
Não é possível garantir que $n^2 + 8$ seja um número primo se $n$ é um múltiplo de 3 e ímpar. Existem exemplos onde $n^2 + 8$ é primo, mas também exemplos onde $n^2 + 8$ é um número composto (não primo)."

Nesse intervalo de um mês a IA "foi à escola" e fez um pequeno curso de TN e de redação. O texto está quase perfeito, inclusive do ponto de vista da lógica matemática (quanto à gramática, ainda usa "onde" de forma errada, o que não deve ser muito grave, acho eu). Cometeu um erro de fatoração, escrevendo $?\, 737 = 19 * 37$, quando o certo é $737 = 11 \cdot 67$. Para mim esse erro foi uma surpresa. Repetindo a pergunta um mês depois, a IA deu mais detalhes, mas continuou apresentando essa fatoração equivocada. □

## 12.8 Problemas

Faça muitas perguntas para sua IA preferida. Lembre-se apenas de que ela é rápida mas não é mais inteligente e criativa do que você.

Fim. Grato.

# Apêndice A

# Lista dos primos até 2500

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 2 | 3 | 5 | 7 | 11 | 13 | 17 | 19 | 23 | 29 | 31 | 37 |
| 41 | 43 | 47 | 53 | 59 | 61 | 67 | 71 | 73 | 79 | 83 | 89 |
| 97 | 101 | 103 | 107 | 109 | 113 | 127 | 131 | 137 | 139 | 149 | 151 |
| 157 | 163 | 167 | 173 | 179 | 181 | 191 | 193 | 197 | 199 | 211 | 223 |
| 227 | 229 | 233 | 239 | 241 | 251 | 257 | 263 | 269 | 271 | 277 | 281 |
| 283 | 293 | 307 | 311 | 313 | 317 | 331 | 337 | 347 | 349 | 353 | 359 |
| 367 | 373 | 379 | 383 | 389 | 397 | 401 | 409 | 419 | 421 | 431 | 433 |
| 439 | 443 | 449 | 457 | 461 | 463 | 467 | 479 | 487 | 491 | 499 | 503 |
| 509 | 521 | 523 | 541 | 547 | 557 | 563 | 569 | 571 | 577 | 587 | 593 |
| 599 | 601 | 607 | 613 | 617 | 619 | 631 | 641 | 643 | 647 | 653 | 659 |
| 661 | 673 | 677 | 683 | 691 | 701 | 709 | 719 | 727 | 733 | 739 | 743 |
| 751 | 757 | 761 | 769 | 773 | 787 | 797 | 809 | 811 | 821 | 823 | 827 |
| 829 | 839 | 853 | 857 | 859 | 863 | 877 | 881 | 883 | 887 | 907 | 911 |
| 919 | 929 | 937 | 941 | 947 | 953 | 967 | 971 | 977 | 983 | 991 | 997 |
| 1009 | 1013 | 1019 | 1021 | 1031 | 1033 | 1039 | 1049 | 1051 | 1061 | 1063 | 1069 |
| 1087 | 1091 | 1093 | 1097 | 1103 | 1109 | 1117 | 1123 | 1129 | 1151 | 1153 | 1163 |
| 1171 | 1181 | 1187 | 1193 | 1201 | 1213 | 1217 | 1223 | 1229 | 1231 | 1237 | 1249 |
| 1259 | 1277 | 1279 | 1283 | 1289 | 1291 | 1297 | 1301 | 1303 | 1307 | 1319 | 1321 |
| 1327 | 1361 | 1367 | 1373 | 1381 | 1399 | 1409 | 1423 | 1427 | 1429 | 1433 | 1439 |
| 1447 | 1451 | 1453 | 1459 | 1471 | 1481 | 1483 | 1487 | 1489 | 1493 | 1499 | 1511 |
| 1523 | 1531 | 1543 | 1549 | 1553 | 1559 | 1567 | 1571 | 1579 | 1583 | 1597 | 1601 |
| 1607 | 1609 | 1613 | 1619 | 1621 | 1627 | 1637 | 1657 | 1663 | 1667 | 1669 | 1693 |
| 1697 | 1699 | 1709 | 1721 | 1723 | 1733 | 1741 | 1747 | 1753 | 1759 | 1777 | 1783 |
| 1787 | 1789 | 1801 | 1811 | 1823 | 1831 | 1847 | 1861 | 1867 | 1871 | 1873 | 1877 |
| 1879 | 1889 | 1901 | 1907 | 1913 | 1931 | 1933 | 1949 | 1951 | 1973 | 1979 | 1987 |
| 1993 | 1997 | 1999 | 2003 | 2011 | 2017 | 2027 | 2029 | 2039 | 2053 | 2063 | 2069 |
| 2081 | 2083 | 2087 | 2089 | 2099 | 2111 | 2113 | 2129 | 2131 | 2137 | 2141 | 2143 |
| 2153 | 2161 | 2179 | 2203 | 2207 | 2213 | 2221 | 2237 | 2239 | 2243 | 2251 | 2267 |
| 2269 | 2273 | 2281 | 2287 | 2293 | 2297 | 2309 | 2311 | 2333 | 2339 | 2341 | 2347 |
| 2351 | 2357 | 2371 | 2377 | 2381 | 2383 | 2389 | 2393 | 2399 | 2411 | 2417 | 2423 |
| 2437 | 2441 | 2447 | 2459 | 2467 | 2473 | 2477 | | | | | |

O próximo primo é 2503.

# Apêndice B

# Respostas e sugestões a alguns problemas

**Observações:** Nem sempre as respostas dadas estão completas. Fique atento ao enunciado do problema para ver se é necessário completar. Muitas vezes não apresentamos nenhum argumento, o que significa que ficou por conta do estudante. Portanto, muitas respostas devem ser vistas apenas como dicas. Lembramos que, na resolução de um problema, apenas encontrar a resposta correta não é suficiente. O processo de descoberta e uma justificativa adequada são muito importantes, e o estudante deve aprender a descrevê-los. Examine bem os exemplos que demos no texto, eventualmente eles podem servir de inspiração.

### Problemas 1.8

1.8.1 (F) (V) (F) (F) (F)

1.8.2 Foi verificado o número de cabelos.

1.8.3 Ele pode fazer uma correspondência um a um entre o conjunto de pedrinhas e o conjunto das ovelhas. O jovem pastor não precisa saber contar. Esse não é um sistema de numeração, pois não fornece um método de enumeração dos números naturais.

1.8.4 Numeral; número ou numeral; número (sistema romano) ou numeral; numeral.

1.8.5 (F) (V) (F) (V) (V) (F).

1.8.8 É um sistema de numeração aditivo de base dois. Os vocábulos básicos são: enea e petcheval. A regra do sucessor pode ser descrita da seguinte forma. Se o nome de um número termina com o vocábulo *petcheval*, o nome de seu sucessor se obtém repetindo-se todos os vocábulos *petcheval* e acrescentando-se o vocábulo *enea*. Se o nome de um número termina com o vocábulo *enea*, o nome de seu sucessor se obtém substituindo-se esse vocábulo por *petcheval*.

1.8.11 11

1.8.14 4444444442.

1.8.16 Agrupe as unidades de $n$ em grupos com $\beta$ unidades cada, formando a maior quantidade possível de grupos. Seja $q$ o número de grupos. Considere dois casos, um em que não sobram unidades (o resto é zero) e outro em que sobram $r$ unidades, com $r$ menor do que $\beta$. Em cada caso veja como deve ser a representação. A representação é única pois, nessas condições, $q$ e $r$ são únicos.

1.8.18 Vale a existência mas não a unicidade.

1.8.19 9 999 999 e 99999.

### Atividades 1.10

1.10.2 Confira [47].

1.10.3 Por exemplo, contar os fios de cabelo da cabeça de uma pessoa, não só por que os fios são muito finos e muito próximos, mas também pela dificuldade de definir o que contar, pois existem fios minúsculos que estão nascendo. Outros exemplos: contar átomos, partículas sub-atômicas, estrelas de uma galáxia, etc. O fato é que certos fenômenos físicos convenientes servem para o homem criar o conceito de número natural. Mas em

certo momento esse conceito se torna abstrato e não depende mais de fenômenos físicos. Nesse ponto estamos de posse de uma instrumento abstrato que pode ser usado em determinadas situações, e em outras não.

## Problemas 2.3

2.3.1 21; 4; 45. O dígito 5 em 456 é a quantidade de pelotões completos que sobram depois de formados os 4 esquadrões.
2.3.2 a) 1427; b) 7 pedrinhas, 2 dedos abaixados e 10 bois extras. c) $a \times 250 + b \times 50 + c$.
2.3.3 Descreva algebricamente o que acontece em cada um dos casos: i) $a$ qualquer, $b$ qualquer e $0 \leq c \leq 4$ ii) $a$ qualquer, $0 \leq b \leq 3$ e $c = 5$ iii) $a$ qualquer, $b = 4$ e $c = 5$.
2.3.4 (a) Podem ser medidos valores até 5.050 gr, de 50 em 50 gramas. (b) Pode ser dispensado o peso de 500 gr, e podem ser medidos valores até 4.550 gr, de 50 em 50 gramas. (c) No caso de se usar os dois pratos, o sistema é $a \cdot 1000 + c \cdot 200 + d \cdot 100 + e \cdot 50 = (acde)$, com $a \leq 4$ ou ausente, $c = \pm 1$, $c = \pm 2$ ou ausente, $d = \pm 1$ ou ausente, $e = \pm 1$ ou ausente. O sinal "$-$" significa subtração, e, quando ele ocorre, o peso correpondente é colocado no mesmo prato da mercadoria que está sendo pesada. Essa representação resguarda a unicidade e é matematicamente correta para os valores considerados.

## Problemas 2.5

2.5.1 27.
2.5.2 $(abc)_{boi} = 250a + 50b + c$, sendo $a$ qualquer número natural ou ausente, $b \leq 4$ ou ausente e $c \leq 49$ ou ausente. Uma limitação desse sistema é que ele não tem um conjunto finito de símbolos básicos. Os "dígitos" $a$, $b$ e $c$ têm que ser representados por um sistema de numeração auxiliar. Fica para o estudante descrever a regra geral do sucessor.
2.5.3 Não é 19.
2.5.4 A resposta da segunda pergunta não é 1550.
2.5.6 84.
2.5.8 O método vale para qualquer número.
2.5.9 Comece escrevendo a representação algébrica expandida de $q$.
2.5.13 Aqui não estamos perguntando o nome das casas.
2.5.14 48, 49, 50, 51.
2.5.15 16, 61, 106, 45.
2.5.16 Algumas possibilidades de idéias que podem ocorrer: **a)** cento e vinte e cinco; **b)** 125 sapatos (ou, quem sabe, planetas, cada um na sua); **c)** algo mais que uma centena; **d)** uma centena, duas dezenas e cinco unidades; **e)** doze dezenas e cinco unidades; **f)** uma centena mais um quarto; **g)** faltam 25 para 150; **h)** 11 ao quadrado mais 4; **i)** dez dúzias mais cinco; **j)** $5 \times 25$; **k)** $5^3$; **l)** 8.
2.5.17 180. Uma forma de resolver é usar o princípio multiplicativo da combinatória. Outra forma é retirar organizadamente da lista dos números de 100 a 999 aqueles em que comparecem os algarismos 2, 5, 7 e 8.
2.5.20 25 e 76.

## Problemas 2.7

2.7.2 Interprete na base dois.
2.7.3 $(102)_{quatro}$. Você usou apenas a base quatro?
2.7.6 $(BA0)_{doze}$.
2.7.7 Zero comparece $\beta + 1$ vezes, um, $2\beta + 1$ vezes, e cada um dos demais, $2\beta$ vezes.
2.7.8 a) $(10000)_{tres}$; b) $(22222)_{tres}$; c) $(20000)_{tres}$. Você usou apenas a base três?
2.7.9 Existem $\beta^{n-1}(\beta - 1)$ com $n$ dígitos.
2.7.10 d) $(1110011000000111)_{dois}$.
2.7.13 $256 = (100)_{dezesseis}$.
2.7.14 $16777216 = (1000000)_{dezesseis}$ cores ou mais do que 16 milhões.
2.7.15 Se $\beta > 10$ temos $(ab)_\beta = a\beta + b = a(10 + (\beta - 10)) + b = ...$

## Problemas 2.12

2.12.3 $(1; 3; 5; 17)_{maia}$.
2.12.6 2 de R$ 512,00, 3 de R$ 64,00, 2 de R$ 8,00 e 2 de R$ 1,00. As quantidades 2, 3, 2 e 2 são os dígitos da representação de 1234 na base oito.
2.12.9 $a = 2$ e $b = 8$.

2.12.10 $\beta = 7$.
2.12.13 (a) $46 = (1201)_{três}$. Os dígitos são os restos das divisões, tomados na ordem contrária ao do seu aparecimento. (b) $841 = (31021)_{quatro}$.
2.12.14 b) $(1331)_\beta = ((11)_\beta)^3$ para todo $\beta \geq 4$, ou $(1000)_\beta = ((10)_\beta)^3$ para todo $\beta \geq 2$.
2.12.15 a) $109 = 2^6 + 2^5 + 2^3 + 2^2 + 2^0$; $5937 = 2^{12} + 2^{10} + 2^9 + 2^8 + 2^5 + 2^4 + 2^0$; $71861 = 2^{16} + 2^{12} + 2^{11} + 2^7 + 2^5 + 2^4 + 2^2 + 2^0$.
2.12.16 Já sabemos que $\beta^{m-1} \leq a < \beta^m$. Aplique $\log_\beta$ para achar $m$. Uma resposta é $m = \lfloor \ln(a)/\ln(\beta) \rfloor + 1$, em que ln é o logarítmo neperiano. Podemos ainda tomar a aproximação $m \approx \log_\beta(a)$. A notação $\lfloor x \rfloor$ indica o maior inteiro menor ou igual a $x$.
2.12.17 A base que proporciona menor gasto de tempo é $\beta = 2$.
2.12.19 $n10^n - 1_n + n + 1$, em que $1_n = 11\ldots1$ tem $n$ algarismos iguais a 1.
2.12.20 1132.

## Atividades 2.13

2.13.3 Consulte, por exemplo, `https://pt.wikipedia.org/wiki/Categoria:Sistemas_de_numeração`.
2.13.7 Considere quais moedas e quais cédulas você precisa ter em mãos para representar todos os valores.

## Problemas 3.2.4

3.2.4.1 O resultado é $\overline{\text{V}}$CCCVII.
3.2.4.3 Por exemplo, na adição de nove parcelas pode ocorrer "vai oito".
3.2.4.4 A versão longa nem sempre evita o uso do "vai um". Exemplo: $139 + 165$.
3.2.4.7 O algoritmo usual imita o procedimento do ábaco, no qual é melhor começar com as unidades.
3.2.4.11 101060.
3.2.4.12 Os resultados são: $(360)_{sete}$, $(11316)_{sete}$, $(136511)_{sete}$.
3.2.4.13 Os resultados são: $(11342)_{cinco}$, $(152053)_{oito}$, $(14925B)_{doze}$.

## Problemas 3.3.3

3.3.3.1 Seja $m = (a - b) - c$. Temos $m + c = a - b \Rightarrow (m + c) + b = a \Rightarrow (m + b) + c = a \Rightarrow m + b = a - c \Rightarrow m = (a - c) - b$.
3.3.3.2 Adicione $c$ a ambos os lados da relação (3.8).
3.3.3.3 Calcule $[(a - c) + (b - c)] + c$.
3.3.3.6 CDLXXVI.
3.3.3.9 $(52432)_{seis}$, $(55513)_{sete}$, $(62127)_{oito}$, $(110101)_{dois}$.
3.3.3.10 $(537)_{oito}$.

## Problemas 3.4.1

3.4.1.1 a) V b) V c) V d) F.
3.4.1.2 a) $a > b$; b) $c \leq d$.
3.4.1.4 Observe que a segunda sentença é a contrapositiva da primeira, portanto basta provar uma delas.
3.4.1.5 Para a primeira parte, utilize a Lei da Tricotomia.
3.4.1.6 Aplique as identidades da Seção 3.3.1.
3.4.1.14 Em sua redação, verifique se está executando algum procedimento infinitas vezes. Em que situações isso pode ser considerado justificável?

## Problemas 3.5.3

3.5.3.7 $(101101)_{dois}$, $(11111101010111)_{dois}$, $(2132022)_{quatro}$, $(1012223221)_{quatro}$, $(2022546026)_{sete}$.
3.5.3.9 Use o método egípcio. O resultado é MCCCXI.
3.5.3.12 Use mediação (divisão por 2) na coluna da esquerda, e duplicação na coluna da direita. Na mediação despreze os eventuais restos 1. Os números assinalados por * são os ímpares.
3.5.3.16 Funciona para produtos da forma $(a3)_{dez} \times (a7)_{dez}$.
3.5.3.17 Por que o dígito da quarta casa do número procurado é 1?
3.5.3.18 Uma idéia é escrever cada número como soma de potências de 2 e depois multiplicar. Para simplificar use a identidade $2^n + 2^n = 2^{n+1}$.

## Problemas 3.6.3

3.6.3.1 13.
3.6.3.3 Foi fácil o professor perceber o erro, pois $3 \times 23 = 69$, que está longe de 701. O estudante esqueceu de colocar um dígito no quociente logo que abaixou um dígito do dividendo.
3.6.3.4 a) $(43)_{cinco}$; b) $(653)_{sete}$.
3.6.3.6 $(11214)_{cinco}$ resto 1; $(12412)_{cinco}$ resto $(22)_{cinco}$; $(100010)_{dois}$ resto 0; $(612)_{sete}$ resto $(32)_{sete}$; $(4126)_{doze}$ resto 2.
3.6.3.8 a) Se $r \neq s$, sua diferença é um número múltiplo de $b$. b) Use a Lei da Tricotomia para concluir que $r = s$.

## Problemas 3.7.1

3.7.1.3 $7^{n+1}$.
3.7.1.4 A soma é 5.
3.7.1.6 (a) Compare potências convenientes com expoentes iguais.
3.7.1.10 Os valores possíveis de $m$ são 8 e 9.

## Problemas 3.9

3.9.1 Se achar que precisa, reveja o significado do sinal $=$.
3.9.4 Por exemplo, "multiplique o primeiro por 4 e some 6". Ou "Some o primeiro com o último e depois dobre".
3.9.6 Explique por que na base $\beta$ dá certo fazer a prova dos $\beta - 1$.
3.9.8 a) Restaram 4 grosas, 4 dúzias e 4 ovos. b) 5 grosas, 10 dúzias e 11 ovos; sobrarão 2 ovos.
3.9.10 O truque dá certo para bases $\beta$ tais que $2 \leq \beta \leq 10$. Depois de fazer as contas na base decimal, nas colunas em que ocorreu a necessidade de empréstimo, o dígito decimal provisório $\tilde{d}$ deve ser substituído por $d = \tilde{d} - (10 - \beta)$.
3.9.11 A base era 8.
3.9.12 1 marc = 12 pinis e 1 drac = 9 marcs.
3.9.13 Descubra primeiro qual é a relação entre a unidade da representação decimal de $n^5$ com a unidade $a_0$ da representação decimal de $n$. Depois estude todos os casos $a_0 = 0$, $a_0 = 1$, ...
3.9.18 Uma forma é calcular o produto. Outra é aplicar a prova dos nove. O dígito é $d = 7$.
3.9.25 Um número natural menos a soma de seus dígitos resulta sempre um múltiplo de 9.
3.9.26 O octaedro tem oito faces, sendo que a cada face corresponde uma outra face oposta, isto é, ambas situadas em planos paralelos. Cada face é numerada de 1 a 8, com a propriedade de que o valor $a$ de uma face e o valor $a'$ da face oposta satisfazem $a + a' = 9$.
3.9.29 362880 e 201599999798400.
3.9.30 São $a \geq 2$ e $b \geq 2$ com $a > 2$ ou $b > 2$.
3.9.31 Uma idéia é dividir as $n$ moedas em três grupos. Se $N(n)$ é a quantidade de pesagens então $N(n) \leq$ a quantidade de dígitos da representação ternária de $n$. Outra idéia é usar divisão por 2.

## Atividades 3.10

3.10.6 O estudante dividiu cada dígito do dividendo 63787 por 3 em sequência, colocando o resto logo abaixo. Repetiu o procedimento com o número formado pelos restos, colocando os dígitos do quociente na casa apropriada. O procedimento está correto.
3.10.8 Consulte, no Capítulo 12, mais exatamente na página 234, a hierarquia adotada pelo aplicativo Maxima a respeito da ordem nas operações aritméticas.

## Temas para investigação 3.11

3.11.1 a) Supondo $m \geq n$, a soma tem $m$ ou $m + 1$ dígitos. c) O produto tem $m + n - 1$ ou $m + n$ dígitos. d) O quociente tem $m - n$ ou $m - n + 1$ dígitos.
3.11.2 Faça exemplos com números com quantidades de dígitos diferentes para perceber regularidades. Em seguida, faça conjecturas e tente demonstrá-las.
3.11.7 Comece investigando o que ocorre com números de dois dígitos. Construa teoremas.

## Problemas 4.2

4.2.1 Uma solução indutiva a título de exemplo. Somando os termos da primeira linha dá 15, que dividido por 5 dá o termo central da linha. Somando os termos da segunda linha dá 40, que dividido por 5 dá o termo central da linha. Induzimos que, em uma linha qualquer, se dividirmos a soma dos termos por 5 obtemos o termo central. Portanto, se em uma linha a soma é 665, o termo central é 665/5=133. Então os números da linha procurada são 131, 132, 133, 134, 135. Notemos, por outro lado, que o último termo da primeira linha dividido por 5 dá 1, e o último termo da segunda linha dividido por 5 dá 2. Induzimos que, em uma linha qualquer, se dividirmos o último termo por 5, obtemos a ordem da linha. O último termo da linha encontrada é 135, que dividido por 5 dá 27. Portanto a linha encontrada tem a posição 27.
4.2.2 Quantos números tem a linha $n$? Qual o último número de cada linha? Quais são os números da linha $n$? Se $a_1 = 1$, $a_2 = 3$, $a_3 = 7$, ... são os números da coluna do meio, o que é $a_n$?
4.2.3 a) $2k + 1$ b) $8k$ c) $k > 8$.

## Problemas 4.4

4.4.1 a) Uma forma de justificar é usar o Método da Indução Completa. Outra forma, mais simples, é observar que, em qualquer progressão aritmética, a soma de dois termos equidistantes dos extremos é constante e igual a $a_1 + a_n$. Chamando $S = a_1 + a_2 + \cdots + a_n$, calcule $2S$. c) Primeiro arrume uma forma de contar os termos da sequência.
4.4.2 a) Calcule $T_{20}$ pelos três métodos para observar bem as diferenças.
4.4.3 A figura sugere $Q_n = T_n + T_{n-1}$ para todo $n \geq 1$ (definindo $T_0 = 0$). Demonstre usando a fórmula de $T_n$.
4.4.4 Usando gnômons sucessivos com 2, 4, 6, ... pontos percebemos que $2 + 4 + \cdots + 2n = n(n + 1)$. Para demonstrar use progressões aritméticas, ou algum resultado obtido anteriormente, ou o Método da Indução Completa.
4.4.7 Note que se $t = T_n$ então $9T_n + 1 = T_{3n+1}$. Para generalizar, observe que a sequência 9, 25, 49, ... é formada pelos quadrados dos ímpares. Que sequência é 1, 3, 6, ...?
4.4.8 Examine os casos $1^3$, $2^3$, $3^3$, e induza uma fórmula. Demonstre em seguida.
4.4.9 a) Escreva $P_n$ como a soma dos $n$ termos de uma progressão aritmética.

## Problemas 4.6

4.6.1 $b \neq 0 \Rightarrow a + b$ tem mais unidades do que $a$.
4.6.3 Use o truque $n \times 0 = n \times (0 + 0) = \ldots$ e o resultado do Problema 4.6.1.
4.6.4 Sejam 0 e $0'$ antecessores de 1. Mostre que $0 = 0'$.
4.6.5 Dado $a^2 = a$ passe $a$ para o outro lado. Use a Lei da Integridade.
4.6.6 Dado $ac = bc$ passe $bc$ para o outro lado.
4.6.8 Dado $ab = a$ passe $a$ para o outro lado.

## Problemas 4.8

4.8.1 Para os pitagóricos, os números pares são da forma $n = q + q$, que coincide com a nossa forma $n = 2q$. Os números ímpares são "os outros". Você está convencido de que "esses outros" são da forma $n = 2q + 1$ ?
4.8.2 Uma observação. Sejam $a = 2m$ e $b = 2n$ números naturais pares. Para fazer a subtração $a - b$ supomos que $a \geq b$. Mostre que isso implica que $m \geq n$ de modo que $t = m - n$ seja um número natural.
4.8.4 Uma dica. Mostre primeiro que a soma de números pares é par, qualquer que seja a quantidade de números.
4.8.6 Elabore uma justificativa geral usando notação algébrica.
4.8.8 Existe uma relação desse problema com o Problema 2.5.9.
4.8.10 Uma condição necessária e suficiente para que o produto $n_1 n_2 \cdots n_s$ termine em zero é que um dos números $n_1$, $n_2$, ..., $n_s$ termine em zero ou que um deles seja par e outro termine em 5.
4.8.13 Expanda e simplifique $(n + 1)^3 - n^3$ ou use 4.8.6.
4.8.16 $6n + 3$.
4.8.21 Divida os números por 3 e considere os casos: (i) existem três números com restos iguais; (ii) não existem três números com restos iguais.
4.8.24 Expanda $111\ldots1$ e note que $10^n = 2^n 5^n$.

## Problemas 4.10

4.10.7 O melhor método que temos até agora para verificar a primaridade de um número $p > 2$ ímpar é: dividi-lo pelos números ímpares $a$ tais que $1 < a < p$; se nehuma divisão for exata, $p$ é primo.

4.10.8 Se $a+b=cq$ e $a=ct$ prove que $q \geq t$.
4.10.9 Dê um exemplo para mostrar que a hipótese $c \neq 0$ é necessária.
4.10.10 9 e 105.
4.10.11 Depois de 11 o menor primo dessa forma é 11111111111111111 (19 dígitos 1's).
4.10.12 Use a definição de primo 4.19 ou o Problema 4.10.3.
4.10.14 $n$ é par.
4.10.18 Existem quatro.
4.10.19 Escreva $n=ab$, com $a \geq b > 1$. Considere separadamente os casos $a=b$ e $a>b$.
4.10.20 Use que número $7^2$ se escreve como um produto de dois números naturais de três maneiras (considerando também a ordem dos fatores). A resposta é $y=24$ e $z=25$.
4.10.23 Com até dois dígitos os únicos múltiplos de 50 são zero e 50. Com três dígitos ou mais são aqueles que terminam em 00 ou em 50.
4.10.24 Use que se $a-7t=b$ então $a$ é múltiplo de 7 se e somente se $b$ é múltiplo de 7.
4.10.25 É claro que se um número natural é múltiplo de 6 então ele é múltiplo de 2 e de 3. Reciprocamente, seja $a$ um número natural múltiplo de 2 e de 3. Por ser múltiplo de 3 temos $a=3t$ para algum número natural $t$. O que podemos afirmar sobre $t$?

## Problemas 4.12

4.12.1 Use classes módulo três.
4.12.2 A palavra "exatamente" colocada no enunciado significa que um dos números é múltipo de 4 e o outro não é.
4.12.3 $m^n$ é par se e somente se $m$ é par e $n \geq 1$. $m^n$ é ímpar se e somente se $n=0$ e $m \geq 1$ ou então se $n \geq 1$ e $m$ é ímpar.
4.12.4 Em geral, quando se obtém uma fórmula algébrica através de uma figura ou de alguns exemplos particulares, se faz uma indução.
4.12.5 Primeiro induza uma fórmula examinando alguns números pentagonais. Em seguida faça uma verificação algébrica da fórmula. É possível também obter uma fórmula combinando fórmulas vistas no texto.
4.12.6 Escreva $2(T_1+T_2+T_3+\cdots+T_n)=T_1+(T_1+T_2)+(T_2+T_3)+\cdots+(T_{n-1}+T_n)+T_n$ e em seguida use 4.4.3 e 10.5.6. A soma é $n(n+1)(n+2)/3$.
4.12.7 Considerando que o $n$-ésimo conjunto tem $n$ números, quantos números gastamos para escrever $n$ conjuntos? Com isso você pode obter o último número do $n$-ésimo conjunto.
4.12.8 O que ocorre com a quantidade de pares e de ímpares na lousa depois de cada operação de substituição?
4.12.9 Suponha que exista a estrada retilínea adicional. A reta determinada por essa estrada divide o plano em dois semiplanos. Estude a localização das cidades nesses semiplanos.
4.12.10 Uma observação simples é que a soma dos números com sinal $-$ deve ser igual à soma dos números com sinal $+$. Ajuda?
4.12.11 Quantos botões trocam de cor a cada vez que se aperta um botão?
4.12.12 Uma dica é: faça uma troca por vez.
4.12.13 Também é impossível, mas o argumento precisa ser outro.
4.12.14 Não é possível. Para justificar use par e ímpar.
4.12.16 Uma solução é $7373=77^2+38^2$.
4.12.19 1000 não é possível, 1001 sim.
4.12.20 Pinte os cubinhos de branco e preto de forma conveniente, ou enumere-os de forma conveniente.
4.12.22 Para ver que A) $\Rightarrow$ B), se $n$ é par considere $n-2$, e se é ímpar, $n-3$. Para ver que B) $\Rightarrow$ A), dado $n>2$ par, aplique B) a $n+2$. Foi demonstrada recentemente pelo matemático peruano Harald A. Helfgott a conjectura fraca de Goldbach, que estabelece que *Todo número natural ímpar* $>5$ *é soma de três primos (não necessariamente diferentes)*

## Temas para investigação 4.14

4.14.1 Examine alguns números representados na base três e procure regularidades relacionadas à sua paridade. Faça conjecturas gerais e as demonstre. Em seguida generalize os resultados para sistemas posicionais em qualquer base.
4.14.2 Observe regularidades nos restos e nos quocientes das divisões. Ache uma fórmula geral. Uma recíproca pode ser: Se o resto da divisão por 8 do quadrado de um número é 1, então o número é ímpar. O que se pode afirmar sobre $8t+1$, em que $t$ é um número triangular?
4.14.3 O dígito da unidade de um produto de números depende de que?

4.14.4 O que ocorre com a quantidade de pares e de ímpares na lousa depois de cada operação de substituição?
4.14.5 Como deve ser a soma dos números de 1 a $n$ para que seja possível realizar o que foi pedido?
4.14.6 a) Depois de cada retirada e respectiva recolocação, o que ocorre com a paridade da quantidade de bolas de cada cor?
4.14.7 b) Dado $n^3$, qual é a forma do primeiro número que aparece na sequência de ímpares? E qual é a forma do último? Como podem ser somados os números dessa sequência? d) Existem muitas. Uma deles é o surpreendente Teorema de Nicômaco: para todo número natural $n$ se tem $(1+2+\ldots+n)^2 = 1^3+2^3+\ldots+n^3$.
4.14.9 Considere separadamente números pares e ímpares.
4.14.12 Lembre-se de que se $n = bq + r$, com $r < b$, então existem $q$ múltiplos de $b$ de 1 a $n$.

## Problemas 5.3

5.3.3 Para justificar c), d) e e) pode-se usar o Teorema Fundamental da Aritmética, que será visto no Cap. 7. f) primo; g) primo ou quadrado do primo menor divisor de $n$.
5.3.5 2520.
5.3.6 128.
5.3.7 a) são os múltiplos de 20; b) 25500.
5.3.8 3000.
5.3.10 vinte. Usando vários resultados anteriores observe primeiro que se $n^2$ é múltiplo de 3, 4 e 5 então $n$ é múltiplo de 3, 2 e 5, portanto de 30.
5.3.11 8.
5.3.14 Como 1 é raiz de $x^3-1$ então $x-1$ é um divisor de $x^3-1$.
5.3.16 Ao construir exemplos para perceber regularidades, sempre represente $n!$ pelo produto com que é definido, e não pelo seu valor numérico.
5.3.18 Use que todo par $> 2$ é composto.
5.3.19 Demonstre a sentença contrapositiva.
5.3.20 a) Use par e ímpar. b) Decomponha o trinômio como produto de dois polinômios com todos os coeficientes inteiros. c) Considere as classes de $p$ módulo 3. d) Sim. Especifique.
5.3.24 Em b), para demonstrar que 2 é o único primo divisor de $2^j$, use contradição.
5.3.25 Para a segunda parte, use contradição.
5.3.26 $n = 5832$. Não se esqueça de demonstrar que os únicos divisores primos de $n$ são 2 e 3. Dentre outras coisas.

## Problemas 5.5

5.5.1 a) primo; b) 3; c) primo; d) 13.
5.5.4 Existem cinco.
5.5.7 a) $\mathcal{A}(n) = (n-3)/2$. b) Seja $[\sqrt{n}\,]$ a parte inteira de $\sqrt{n}$. Se $[\sqrt{n}\,]$ é ímpar, temos $\mathcal{A}(n) = \frac{[\sqrt{n}]-1}{2}$; se $[\sqrt{n}\,]$ é par, temos $\mathcal{A}(n) = \frac{[\sqrt{n}]-2}{2}$. c) 499. Não é necessário fazer as contas, 1 000 003 é primo.

## Problemas 5.7

5.7.1 $91 = 7 \cdot 13$.
5.7.2 a) Existem 62 primos $\leq 300$. Confira sua lista com a da página 243. Para facilitar, você consegue programar o crivo em algum aplicativo, quem sabe uma planilha digital? b) $273 = 3 \cdot 7 \cdot 11$. c) Existem 8 divisores.
5.7.3 a) Para explicar use classes módulo 6.
5.7.4 b) Ao eliminar $p^2$, o múltiplo seguinte seria $(p+1)p$, que é par, e assim não está na tabela. O múltiplo seguinte é $(p+2)p$, que é ímpar, e está na tabela. E assim por diante, os múltiplos de $p$ que são ímpares, a partir de $p^2 = (p+0)p$, são $(p+2i)p$, $i \geq 1$. Calcule a "distância" entre dois múltiplos ímpares consecutivos (incluindo eles mesmos).
5.7.5 $1\,455\,521 = 61 \cdot 107 \cdot 223$. Incluímos esse número relativamente grande para o estudante "sentir" a dificuldade. Existem aplicativos computacionais algébricos que fazem esse cálculo muito rapidamente. O estudante pode consultar o último capítulo deste texto.
5.7.7 Implemente o crivo na tabela dada na página 141 prestando atenção ao que ocorre com relação à pergunta feita.

## Problemas 5.9

5.9.1 Para comprovar use o Problema Resolvido 5.10.
5.9.3 Qual é a relação de um número $m \leq n$ com $n!$ ?
5.9.5 Use os seguintes fatos: (i) todo número primo ímpar é de uma das duas formas seguintes: $4n+1$ ou $4n+3$; (ii) o produto de números da forma $4n+1$ ainda é dessa forma; (iii) se $a$ e $b$ são números naturais tais que $ab$ é múltiplo de 3, então $a$ é múltiplo de 3 ou $b$ é múltiplo de 3. Agora, se $3 < p_1 < p_2 < \cdots < p_k$ são primos da forma $4n+3$, considere o número $4(p_1 \dots p_k)+3$. Prove que ele tem um divisor primo $p$ da forma $4n+3$ diferente dos anteriores.

## Problemas 5.11

5.11.5 1
5.11.6 Divida $12k+10$ por $3k+2$. Resposta: 1 se $k$ for ímpar, e 2 se for par.
5.11.14 21
5.11.15 37
5.11.16 A relação que temos em mente é que os divisores comuns de $a$ e $b$ coincidem com os divisores de $\text{mdc}(a,b)$. Para demonstrar use o algoritmo euclidiano aplicado a $a$ e $b$.
5.11.17 7
5.11.20 O resultado que temos em mente é: "Se $p$ e $q$ são primos diferentes e se $p$ divide $tq$, então $p$ divide $t$, qualquer que seja o número natural $t$." Confira o Capítulo 7. Usando esse resultado demonstre a afirmação sugerida no problema.
5.11.21 A propriedade que temos em mente é $\text{mdc}(a,b)\,\text{mmc}(a,b) = ab$.

## Problemas 5.13

5.13.1 Para a parte a) use a fórmula do binômio.
5.13.2 Apenas para $n = 1$.
5.13.4 Refere-se aos números da forma $(ddd...d)_{dez}$.
5.13.5 Apenas para $n = 1$.
5.13.6 Comece escrevendo $8 = 2^3$. Em seguida use a identidade 5.4.
5.13.8 Existem.
5.13.9 O resto é sempre 2.
5.13.10 Se $n = 1$, $a-1$ é primo. Se $n \geq 2$, temos $a = 2$ e $n$ é primo.
5.13.12 2 é o único primo que é soma de dois cubos.
5.13.13 2 é o único primo que é soma de duas potências quínticas.

## Problemas 5.15

5.15.1 $a = 5$ e $b = 4$.
5.15.2 Sete possibilidades. Para ajudar use uma tabela de primos ou um aplicativo computacional algébrico.
5.15.3 15. Sugestão: use o seguinte esquema para etiquetar os números das faces: $a$ e a face oposta $b$; $n$ e a face oposta $m$, e $x$ e a face oposta $y$.
5.15.5 Uma providência útil é testar o procedimento para alguns números, por exemplo, $p = 7$, $p = 25$ e $p = 35$.
5.15.6 Use a propriedade (v) do Problema 5.11.2.
5.15.7 Considere classes módulo 6. Quais são as condições sobre um número natural qualquer para que seja válida a afirmação?
5.15.8 $\text{mdc}(84,90) = 2 \cdot 3 = 6$, $\text{mmc}(84,90) = 2^2 \cdot 3^2 \cdot 5 \cdot 7 = 1260$, $\text{mdc}(1001,4235) = 7 \cdot 11 = 77$, $\text{mmc}(1001,4235) = 5 \cdot 7 \cdot 11^2 \cdot 13 = 55055$, $\text{mdc}(20,30,14) = 2$ e $\text{mmc}(20,30,14) = 2^2 \cdot 3 \cdot 5 \cdot 7 = 420$.
5.15.10 Essa variante pode não funcionar para três números (ou mais). Arrume um contra-exemplo.
5.15.15 Justifique por que se obtém a reposta com o uso do mdc.
5.15.18 3 voltas da engrenagem maior e 4 da menor.
5.15.19 Justifique por que o mmc fornece a reposta.
5.15.21 A diagonal intercepta uma vez cada uma das $n+1$ retas horizontais e uma vez cada uma das $m+1$ retas verticais. Entre duas interseções consecutivas a diagonal passa pelo interior de um quadrado unitário. Assim, a princípio seriam $n+1+m+1$ interseções. Mas devemos subtrair as interseções comuns a uma linha vertical com uma linha horizontal, para que elas não sejam contadas duas vezes. Quantas são?
5.15.22 a) Use o resultado do Problema 5.3.24(a).

5.15.23 Comece mostrando que todo número natural $\ell$ se escreve na forma $\ell = 2^h 3^g b$ para números naturais $h$, $g$ e $b$, sendo $b$ não múltiplo de 2 e nem de 3.

## Temas para investigação 5.16

5.16.1 Sugestões: Demonstre que a afirmação não vale para qualquer $m$ composto. Reestude os casos $m = 2$ e $m = 3$ (cf. Problema 4.8.23). Usando método semelhante ao do caso $m = 3$, demonstre que a afirmação vale para $m = 7$ (para $m = 5$ também vale, e é muito fácil constatar). Encaminhe uma demonstração para $m$ primo qualquer.
5.16.3 Dado $2 \le n \le 120$, se $n$ não é múltiplo de 7 e se o resto da divisão de $n$ por 30 for 1 ou primo $> 5$, então $n$ é primo. Decorando os primos $\le 30$ (ou dado $7 \le p \le 30$ aplique um critério de divisibilidade por 2, 3 ou 5, pois se $p$ não for primo ele é divisível por 2, 3 ou 5). Dado $31 \le n \le 120$, aplicando a regra, temos à mão todos os primos $\le 120$. Ao justificar o teste, lembre-se de que $7^2 = 49 > 30$ e $11^2 = 121 > 120$.
5.16.4 8 051 é próximo de qual quadrado perfeito?
5.16.5 Para algumas demonstrações veja se ajuda escrever $1_n = \frac{1}{9}(10^n - 1)$.
5.16.7 Uma regularidade evidente é: $7 \in \mathcal{D}(2^j - 1)$ se e somente se $j$ é múltiplo de 3. Você pode provar isso.
5.16.12 O esquema do algoritmo pode ser:
*Passo 0.* Dado $n \ge 5$ ímpar, assinale $x = [\sqrt{n}\,]$; se $x^2 = n$, pare e $n$ é composto; caso contrário faça $x \to x + 1$.
*Passo 1.* Enquanto $x \le (n + 1)/2$, assinale $y = \sqrt{x^2 - n}$; se $y$ for inteiro, pare; caso contrário faça $x \to x + 1$.

Se $x < (n + 1)/2$ então $n$ é composto, e $x + y$ e $x - y$ são fatores. Se $x = (n + 1)/2$ então $n$ é primo. Para uma demonstração confira [24] a partir da página 40. Usando uma calculadora e seguindo o algoritmo passo a passo obtemos $302\,303 = 503 \cdot 601$.

## Problemas 6.3

6.3.3 Se um número natural (em sua representação decimal) termina com 2, 3, 7 ou 8, podemos afirmar que ele não é um quadrado perfeito.
6.3.4 Suponha que seja possível. Usando que os números são ímpares, verifique que a soma de seus quadrados tem resto 2 módulo 4. Por outro lado, essa soma é par, e, se ela for um quadrado, seu resto módulo 4 é zero. Como o resto é único, temos uma contradição.
6.3.5 R.
6.3.6 H.
6.3.7 Comece escrevendo $n = 11q + r$, $0 \le r < 11$.
6.3.10 **a)** $n = 5q + 3$; **b)** Nenhum.

## Problemas 6.5

6.5.2 Os sistemas de numeração aditivos estão definidos na Seção 1.6.

## Problemas 6.6

6.6.1 Não.
6.6.2 O percurso total da pista é de 13 km. Se $d$ é o percurso da corrida desejada, divida $d$ por 13.
6.6.3 Os pares.
6.6.4 Utilize classes módulo três.
6.6.5 Utilize as classes $a$ módulo quatro e $n$ módulo 2.
6.6.7 b) Escreva $x = m + y$, sendo $y$ um número real tal que $0 \le y < 1$. Em seguida faça a divisão euclidiana de $m$ por $n$, e calcule as duas expressões.
6.6.8 d) Use que a quantidade de números de 1 a $n - 2$ (portanto, também de 2 a $n - 2$) que são múltiplos de 2, 3 ou 5 é $\lfloor \frac{n-2}{2} \rfloor + \lfloor \frac{n-2}{3} \rfloor + \lfloor \frac{n-2}{5} \rfloor - \lfloor \frac{n-2}{2\cdot 3} \rfloor - \lfloor \frac{n-2}{2\cdot 5} \rfloor - \lfloor \frac{n-2}{3\cdot 5} \rfloor + \lfloor \frac{n-2}{2\cdot 3\cdot 5} \rfloor$. f) 265.
6.6.9 Comece com a Proposição 5.22.
6.6.11 **a)** Observe que essa representação consiste do sistema sexagesimal com três casas e com o dígito da casa três limitado por 24. **b)** 20h20m3s; 17h40m26s; 21h52m51s; 1h39m25s.
6.6.12 a) A forma expandida é $60^2 \cdot 360u + 60^2 x + 60y + z$, sendo $0 \le z < 60$, $0 \le y < 60$, $0 \le x < 360$ e $0 \le u$. É um sistema posicional, conforme o resultado do Problema 6.6.14. b) $6^v 8° 26' 21''$.
6.6.13 a) Se $a = 2$, escreva $a = 3 - 1$, e esta é a forma requerida. Suponha $a \ge 3$. Seja $a = \tilde{q}_1 3 + \tilde{a}_0$, com $\tilde{a}_0 = 0$, 1 ou 2. Se $\tilde{a}_0 = 0$ ou 1 tome $a_0 = \tilde{a}_0$ e $q_1 = \tilde{q}_1$. Se $\tilde{a}_0 = 2$ tome $a_0 = -1$ e $q_1 = \tilde{q}_1 + 1$, e temos $a = q_1 3 - 1$. Em qualquer caso temos $a = q_1 3 + a_0$, com $a_0 = 1$, 0 ou $-1$. Prove que $q_1 < a$. Depois repita o processo para $q_1$, e assim sucessivamente.

6.6.14 Imite a demonstração do Teorema 6.7. Comece com o caso infinito. Para o caso finito, seja $\beta_0 = 1 < \beta_1 < \beta_2 < \beta_3 < \ldots < \beta_m$ uma sequência finita de números naturais. Dado $n \geq 1$, se $n \geq \beta_m$, acrescente à sequência o termo $\beta_{m+1} = n + 1$. Tudo funciona como no caso infinito.

## Temas para investigação 6.7

6.7.1 Sugestão: observe primeiro que a unidade de $a^n$ só depende da unidade $a_0$ de $a$. Examine separadamente os casos $a_0 = 0$, 1, 2, ..., 9.
6.7.3 a) Uma conjectura é: $7 \nmid 2^n + 1$. Para demonstrar considere $n$ módulo 3. Use que $7 \mid 2^{3q} - 1$. Outras conjecturas podem ser feitas.

### Problemas 7.3

7.3.1 Use contradição.
7.3.2 Aplique o Teorema 7.7.
7.3.7 c) São exatamente todos os primos $\leq 91$.
7.3.15 A afirmação vale para $n = 1$ e para os números compostos $n > 4$.
7.3.16 Considere $i!\binom{p}{i}$.

### Problemas 7.5

7.5.2 $m = 35$
7.5.3 Isso já foi feito antes, mas agora use o TFA.
7.5.5 Dica: se $n^3 = m^2$, então nas decomposições canônicas de $n$ e $m$ comparecem exatamente os mesmos primos.
7.5.8 a) Imite a demonstração do Teorema 4.22.

### Problemas 7.7

7.7.1 $\text{mmc}(1, 2, 3, 4, 5, 6, 7, 8, 9, 10) = 5 \cdot 7 \cdot 8 \cdot 9 = 2520$.
7.7.3 Use o Problema 7.5.3.
7.7.5 Uma condição é que os números $a_1$, $a_2$, ..., $a_\ell$ sejam relativamente primos dois a dois. Outra condição suficiente é que $a_1 = a_2 = \ldots = a_\ell$ e, nesse caso, qual é a condição sobre $\ell$ e $k$?
7.7.7 Use 7.2 e 7.18.
7.7.10 Use 7.18, 7.3.12 e 3.6.3.7.
7.7.11 a) Para provar que $\mathcal{M}(a) \cap \mathcal{M}(b) \subseteq \mathcal{M}(\text{mmc}(a, b))$, seja $m = as = bt \in \mathcal{M}(a) \cap \mathcal{M}(b)$. Considere $d = \text{mdc}(a, b)$, com $a = a_1 d$ e $b = b_1 d$ e $\text{mdc}(a_1, b_1) = 1$. Manipulando as identidades chegamos a $m = \frac{ab}{d} s_1 = \text{mmc}(a, b) s_1$.
7.7.12 Dado $11 \leq p \leq 99$, temos $\sqrt{p} \leq 10$. Se $p$ é composto, ele tem como fator primo 3, 5 ou 7. Logo $\text{mdc}(3 \cdot 5 \cdot 7, p) > 1$.
7.7.13 Para ajudar reestude o Problema Resolvido 6.4, assim como os dois seguintes. O resultado do Problema 6.6.7 b) também pode fornecer um caminho.

### Problemas 7.9

7.9.2 Se quiser use um aplicativo computacional algébrico. No Maxima um número $n$ é perfeito quando o comando divsum(n)-n retorna o próprio $n$.
7.9.3 O programa no Maxima for n:1 thru 10000 do if divsum(n)=2*n then print(n); retorna os números perfeitos $P_1$, $P_2$, $P_3$ e $P_4$, confirmando a primeira parte do Problema. Estendendo o limite de $n$ para 10 000 000 000, verifica-se que até esse limite existem apenas seis números perfeitos
7.9.4 No Maxima use o seguinte programa para calcular os números amigos $\leq 10\,000$: for n:1 thru 10000 do for m:1 thru 10000 do if n<m and divsum(n)-n=m and divsum(m)-m=n then print(n,"e",m,"são amigos;"); Existem cinco pares.

### Problemas 7.10

7.10.2 9.
7.10.6 1.
7.10.7 Use 5.21 e 7.3.16.
7.10.8 Use 5.21 e 7.3.16.
7.10.9 Proceda por contradição.

7.10.10 Considere um sistema de coordenadas cartesianas, de modo que um vértice do retângulo seja $(0,0)$ e o outro, $(a,b)$. Tome a diagonal por esses dois pontos. Escreva $d = \text{mdc}(a,b)$, $a = a_1 d$ e $b = b_1 d$.
7.10.11 O número do armário deve ser um quadrado perfeito para que tenha um número ímpar de divisores.

### Temas para investigação 7.11

7.11.1 Observe que 97 é primo, e o próximo primo é 101. Separe sua investigação em três casos: $1 < n \leq 100$, $100 < n \leq 10\,200$ e $10\,200 < n$.
7.11.2 O menor contra-exemplo para a recíproca foi encontrado por Pierre F. Sarrus em 1819. De $n = 2$ a $n = 1000$ só existem três contra-exemplos. Use um aplicativo computacional algébrico para encontrá-los. No Maxima pode usar for n from 2 thru 1000 do if not primep(n) and mod(2^n-2,n)=0 then print(n);
7.11.3 Faça experimentos numéricos. Uma ideia é considerar $p$ módulo 8.
7.11.4 Comece escrevendo $n = 2^k b$ e use identidades.
7.11.5 De que forma são os primos que aparecem?

### Problemas 8.3

8.3.2 $(0,t,t)$ e $(t,0,t)$, para todo número natural $t$.
8.3.3 **d)** Se $r = m/n$ temos $v = (m^2-n^2)/2mn$ e $w = (m^2+n^2)/2mn$. Se $m > n > 0$ obtemos o terno pitagórico $(2mn, m^2-n^2, m^2+n^2)$.
8.3.5 **a)** $(5,12,13)$. **b)** $(3,4,5)$ e $(7,24,25)$. **c)** $(n,(n^2-1)/2,(n^2+1)/2)$. **d)** $(n,(n^2-4)/4,(n^2+4)/4)$.

### Problemas 8.5

8.5.2 Os casos possíveis são três.
8.5.3 Para mostrar que $xy$ é múltiplo de 3 use classes módulo 3 e que nenhum quadrado é da forma $3k+2$.
8.5.4 Seja $(x,y,z) = (2kmn, k(m^2-n^2), k(m^2+n^2))$. Se $m$ ou $n$ é múltiplo de 5 então $5 \mid x$. Caso contrário, $m^2 = 5l+1$ ou $m^2 = 5l-1$, o mesmo para $n^2$. Examine todos os casos.

### Problemas 8.7

8.7.3 Note que $x = (n+1)/2$ e $y = (n-1)/2$ constituem uma solução de $x^2 - y^2 = n$. Suponha que $n = ab$ seja composto. Então $x = (a+b)/2$ e $y = (a-b)/2$ são números naturais e constituem uma solução de $x^2 - y^2 = n$ diferente da anterior. Reciprocamente, suponha que a equação dada tenha mais de uma solução. Seja $(c,d) \neq ((n+1)/2,(n-1)/2)$ uma segunda solução. Como $n = (c+d)(c-d)$, prove que $c-d > 1$.

### Temas para investigação 8.8

8.8.1 c) Use a fórmula de Heron para calcular a área de triângulos. d) Restrinja os valores de $x$, $y$ e $z$ a famílias adequadas para que a área seja um número natural e para que sejam medidas de lados de triângulos. Uma ideia é começar com $x = y$.

### Problemas 9.4

9.4.4 Examine quatro casos, conforme cada um dos números $a$ ou $b$ esteja ou não em $\mathbb{N}$.
9.4.5 Examine oito casos, conforme cada um dos números $a$, $b$ ou $c$ esteja ou não em $\mathbb{N}$.
9.4.6 Examine oito casos, conforme cada um dos números $a$, $b$ ou $c$ esteja ou não em $\mathbb{N}$.
9.4.7 Examine quatro casos, conforme cada um dos números $a$ ou $b$ esteja ou não em $\mathbb{N}$.
9.4.10 Examine quatro casos, conforme cada um dos números $a$ ou $b$ esteja ou não em $\mathbb{N}$.

### Problemas 9.6

9.6.1 Seja $S \subset \mathbb{N}$ um subconjunto com as seguintes propriedades: (i) $0 \in S$; (ii) se $n \in S$ então $n+1 \in S$. Suponha $S \neq \mathbb{N}$. Seja $A = \mathbb{N} - S$. Tomando o mínimo de $A$, obtenha uma contradição.

### Problemas 9.8

9.8.4 $n = -15$, $m = -73$. O mdc é 19.
9.8.6 a) 1; b) 1 ou 17. Determine a forma de $k$ para que seja 17.
9.8.7 $x = 2 \cdot 3^2$ e $y = 2^3 3^2$ ou o contrário.
9.8.8 Comece observando que se $p/q$ for uma possível raiz, não é perda de generalidade supor que $p$ e $q$ não são ambos pares.
9.8.9 $m = 1125$.
9.8.10 1.

**Problemas 9.9**

9.9.1 Para definir use o mesmo esquema de 3.7. Também pode ser: para quaisquer inteiros $a > 0$ e $n \geq 0$, seja $(-a)^n = a^n$ se $n$ for par, e $(-a)^n = -a^n$ se $n$ for ímpar.
9.9.2 c) Uma solução é $\ell = 0$, $m = 5$ e $n = -34$.
9.9.3 A notação $a \mid b$ implica que $a \neq 0$. Examine separadamente os casos $c = 0$ e $c \neq 0$.
9.9.4 $2^9$ ou $2^{12}$. Sugestão: escreva $a$ e $b$ na forma $2^s t$, com $t$ ímpar. Notemos que esse problema não é simétrico em relação a $a$ e $b$, isto é, trocando $a$ por $b$ o resultado não é o mesmo.
9.9.5 $p^6$.
9.9.6 Divida $9a + 5b$ por $2a + 3b$ de forma que o resto seja múltiplo de 17.
9.9.7 Primeiro observe que os números podem ser todos $\geq 2$ sem perda de generalidade. Depois prove que, dados dez inteiros consecutivos, todos $\geq 2$, existe pelo menos um cujos fatores primos são todos $\geq 11$ (para isso use módulo 3). Esse é relativamente primo com cada um dos outros.

**Temas para investigação 9.10**

9.10.1 Para ver que $5 \mid n^9 - n$ para todo $n$, use $n^9 - n = n(n^8 - 1) = n(n^4 - 1)(n^4 + 1)$. Em geral $5 \mid n^{4s+1} - n$.
9.10.2 Considere $q = k(p - 1) + 1$.
9.10.3 a) Uma regularidade: se $q$ é primo e $q \mid 2^p - 1$, então $p \mid q - 1$. É verdadeira. Confira [24], página 156.
9.10.4 a) Mesma dica do problema anterior.
9.10.5 Faça experimentos numéricos para descobrir regularidades.

**Problemas 9.12**

9.12.2 Use que $35 = 5 \cdot 7$.
9.12.3 Como $7^4 \equiv 01 \pmod{100}$, ache $s$ tal que $7^{1000} = 4q + s$.
9.12.4 O resto é 5. Dica: $10^6 \equiv 1 \pmod{7}$.
9.12.6 Aqui é melhor usar um aplicativo computacional algébrico. No Maxima pode ser for n from 0 thru 15 do print(n,".....",mod(3^n,17));
9.12.8 Uma forma é multiplicar a equação por 3.

**Problemas 10.3**

10.3.1 Para verificar que $7 \mid n^7 - n$ uma forma é escrever $n^7 - n = n(n^6 - 1) = n(n-1)(n^2+n+1)(n+1)(n^2-n+1)$ e considerar os casos $n = 7k + r$, $0 \leq r < 7$.
10.3.2 No Maxima use for p from 2 thru 1100 next next_prime(p) do if mod(2^(p-1)-1,p^2)=0 then print(p); Em tempo: 1091 é primo.
10.3.3 Se quiser usar o Maxima um programa é: for n from 1 thru 10^5 do if integerp(sqrt(991*n^2+1)) then print(n); Coloquei como limite $10^5$, pois o limite $12 \cdot 10^{27}$ é muito grande e o aplicativo levaria muito tempo para terminar. Para testar o número n dado simplesmente use integerp(sqrt(991*n^2+1)), que retorna true.
10.3.4 No Maxima use os comandos primep(2^(2^5)+1); e factor(2^(2^5)+1); O número de Fermat para $n = 6$ não é primo.

**Problemas 10.5**

10.5.1 Chame $s_n = 1 + 2 + 2^2 + 2^3 + \cdots + 2^n$, e calcule $s_n - 2s_n$.
10.5.2 $A(n)$ : $n < 2^n$, para todo $n \geq 0$.
10.5.9 Solução 1: Seja $c(n)$ o número de cumprimentos. Existem $n(n-1)$ encontros. Logo $c(n) = n(n-1)/2$, para $n \geq 1$. Não foi necessário o MIC. Solução 2: $c(n) = c(n-1) + n - 1$. Demonstre pelo MIC que $c(n) = \frac{n(n-1)}{2}$, $n \geq 1$. Solução 3: dá para ser mais informal.

**Problemas 10.7**

10.7.1 Considere $A(n)$ : $f_n$ e $f_{n-1}$ são coprimos para todo $n \geq 1$.
10.7.2 Considere $A(n)$ : $3 | f_{4n}$ para todo $n \geq 0$. Dica: $f_{4(n+1)} = 3f_{4n+1} + 2f_{4n}$.
10.7.3 Use o Segundo Princípio da Indução Completa.
10.7.4 Use o Segundo Princípio da Indução Completa.
10.7.5 Use o Segundo Princípio da Indução Completa.

**Problemas 10.8**

10.8.1 c) também usa a).
10.8.2 Uma afirmação que pode ser demonstrada com o MIC é: $A(n)$: a linha $n$ tem $2n - 1$ termos e termina com $n^2$ , para todo $n \geq 1$.

10.8.3 Use $3^{2(n+1)} - 1 = 3^{2n}3^2 - 3^2 + 3^2 - 1$.
10.8.5 Observe que se $A_1A_2 \dots A_{n+1}$ é um polígono convexo, então $A_1A_2 \dots A_n$ também é.
10.8.9 Suponha primeiro $a \geq 0$. Ao demonstrar a tese da indução, use o resultado do Problema 7.3.16.

### Temas para investigação 10.9

10.9.3 Regularidades observadas: 1ª. É muito fácil perceber, use congruências para demonstrar. 2ª. $1 \leq m < n \Rightarrow F_m \mid F_n - 2$. 3ª. Se $m \neq n$ então $\text{mdc}(F_m, F_n) = 1$.

### Problemas 11.5

11.5.2 $(x, y) = (10 - 29t, 1 - 3t)$.
11.5.3 5, 3 e 33.
11.5.4 2, 30 e 68, e mais outras seis soluções.
11.5.5 9 e 71, ou 30 e 40, ou 51 e 9.
11.5.6 18.
11.5.7 $(x, y) = (-1500 + 5t, 1000 - 3t)$ para $300 \leq t \leq 333$. O custo pode ser constante, ou mínimo para as quantidades de 0 e 100 ou 165 e 1.
11.5.8 $100 = 7 \cdot 8 + 11 \cdot 4$.

### Temas para investigação 11.6

11.6.1 Demonstre que o sistema tem solução se, e somente se, $\text{mdc}(a_1, a_2, \dots, a_n) \mid b$.

### Problemas 12.4

12.4.1Use P(n):=n*(3*n-1)/2; map(P, [1, 2, 3, 4, 5, 6, 7, 8, 9, 10]); A resposta é [1,5,12,22,35,51,70,92,117,145].
12.4.2 Usando ifactors(34567); se obtém $34567 = 13^1 2659^1$.
12.4.3 Use o comando primep(n).
12.4.4 Use o comando mod(458941,7) ou divide(458941,7).
12.4.7 Use os comandos factor(n) e divisors(n).

### Problemas 12.6

12.6.1 Uma opção é o bloco de comandos block([P], P:1, for i:1 step 2 while i<=57 do P:P*i, return(P));
12.6.2 Começe com block([REP], REP:1, for i:1 thru 20 do display(i,REP,primep(REP)) and REP:REP+10^i); Para obter um programa que só avalie as rep-unidades que têm um número primo de 1's, defina primeiro por recorrência REP(m):=sum(10^(n-1),n,1,m); depois use for i:1 thru 29 do if primep(i) then display(i,primep(REP(i))); Nessa faixa são primos REP(2), REP(19) e REP(23).
12.6.3 Se quiser pesquisar $2^p - 1$ apenas para $p$ primo (pois se $p$ for composto, $2^p - 1$ é também composto), uma possibilidade é for i:1 thru 23 do if primep(i) then display(i,primep(2^i-1));
12.6.4 Para obter a tabela use for i:1 thru 10 do display(i,factor(REP(i))); depois de definir REP(n). Note que $101 \mid 1111$ e $101 \mid 11111111$, e que $11111111 = 1111x + 1111$. O que é $x$?
12.6.5 Para obter a tabela uma possibilidade é
g(n):=2^n+(-1)^(n+1); for n:1 thru 20 do display(g(n),factor(g(n)));
Melhor:
g(n):=2^n+(-1)^(n+1); for n:1 thru 20 do print("n= ", n,"g(n)= ", g(n), "e ",g(n),"=",factor(g(n)));
Uma regularidade evidente é que 3 é divisor de todos os termos.
12.6.7 $n = 20$. O programa pode ser (o limite n=30 foi escolhido por tentativa): for n:1 thru 30 do if not primep(6*n-1) then if not primep(6*n+1) then display(n);
Melhor: for n:1 thru 30 do if not primep(6*n-1) then if not primep(6*n+1) then print("n=",n, ", ", "6*n-1= ",6*n-1, "não é primo e 6*n+1= ", 6*n+1, "não é primo");
12.6.8 Usei este, mas o limite i<=20 não funcionou como gostaria e assim o limite 260 de n foi colocado por tentativas.
for i from 1 while i<= 20 do for n from 2 thru 260 next next_prime(n) do if primep(n+50) then print("primo",i,": ","n=",n,"n+50=", n+50) and i:i+1;
12.6.9 Usei block([P], P:3, for i from 5 thru 100 next next_prime(i) do P:P*i, return(P)); Use o comando compare(a,b); para comparar a resposta do Maxima com $P$.
12.6.10 Pode usar
for n:0 thru 1729 do for i:1 thru 12 do for j:1 thru 12 do if n=i^3+j^3 and i<=j then print(n,"=",i,"^3","+",j,"^3");
Os limites de i e j são calculados como $[\sqrt[3]{1729}] = 12$. Um programa melhor seria pedir o retorno apenas dos números que têm duas decomposições. As decomposições de 1729 são: $1729 = 1^3 + 12^3 = 9^3 + 10^3$.

# Apêndice C

# Créditos das figuras

**Observação:** As figuras não referidas foram construídos pelo autor com o uso do programa gráfico vetorial Inkscape, ou com o Pictex ou o Tikz, ou ainda com o Geogebra.

## Capa e Apresentação

**Figura da capa externa** Construída pelo autor com o Inkscape.

**Figura da capa interna** Clip Art Inkscape `http://www.openclipart.org/` Autor: Kattekrab. Domínio público. Consultado em outubro de 2010.

## Capítulo 1: A arte de contar

**Figura da página 5:** Clip Art vetorial disponibilizada em `http://all-free-download.com/free-vector/download/a-variety-of-clip-art-books_155211.html` Consultado em 10 de agosto de 2016.

**Figuras da página 6:** Clip Art vetorial disponibilizada em `http://http://publicdomainvectors.org/pt/` Consultado em 14 de setembro de 2016.

**Figura 1.1, página 12:** Detalhe do papiro Rhind obtido em `https://en.wikipedia.org/wiki/Rhind_Mathematical_Papyrus#/media/File:Rhind_Mathematical_Papyrus.jpg` Autor: Paul James Cowie (Pjamescowie). Data: 21 de maio de 2006. Fotografia e texto de domínio público. Consultado em 15 de agosto de 2016.

**Símbolos da Seção 1.7, página 12**: Os desenhos dos símbolos numéricos áticos e jônicos foram obtidos da página *Greek numerals* em `https://en.wikipedia.org/wiki/Greek_numerals` e disponibilizados para domínio público por *Future Perfect at Sunrise* em 14 de julho de 2012. Consultado em 16 de agosto de 2016.

**Figura 1.2, página 13:** Foto de manuscrito grego do Século II obtido em `https://commons.wikimedia.org/wiki/File:P._Lund,_Inv._35a.jpg` O papiro se encontra na Lund University Library e foi escaneado do livro *The Exact Sciences in Antiquity* de Otto E. Neugebauer [85]. Domínio público. Consultado em 17 de agosto de 2016.

**Figura 1.3, página 14:** Foto de relógio hebreu do Século XX adaptado de `https://commons.wikimedia.org/wiki/File:Pocket_watches_with_Hebrew_numerals.JPG` Museu Judaico de Berlim. Disponibilizado em 24 de janeiro de 2015 como domínio público. Consultado em 17 de agosto de 2016.

**Figura 1.4, página 15:** Foto disponível em `https://en.wikipedia.org/wiki/File:Carlos_IV_Coin.jpg` Disponibilizada em 15 de janeiro de 2007 por Coinman62 como domínio público. Consultado em 17 de agosto de 2016.

**Figura 1.5, página 16:** Foto de tablete cretense obtido em `https://commons.wikimedia.org/wiki/File:Cretan_hieroglyphs2.png` Autor: Y-barton. Data: 2 de dezembro de 2013. Direitos de imagem de acordo com o sistema Creative Commons Attribution-Share Alike 3.0. Consultado em 14 de agosto de 2016.

**Foto da página 18:** Recorte de foto de uma estátua de Jean Piaget obtida de `http://www.picswiss.ch/Genf/GE-05-07.html` Os direitos autorais são de propriedade do fotógrafo Roland Zumbühl. Permitido uso privado não comercial. Consultado em dezembro de 2010.

## Capítulo 2: Sistemas de numeração posicionais

**Figura 2.1, página 23:** A lousa do desenho foi disponibilizada em `http://publicdomainvectors.org/pt/vetorial-gratis/Quadro-negro-vetor-clip-art/11718.html` Consultado em 27 de setembro de 2016.

**Figura 2.2, página 24:** Créditos da foto da balança: Lilly_M, CC BY-SA 3.0, via Wikimedia Commons `https://commons.wikimedia.org/wiki/File:Simple_balance_scales-02.jpg` Consultado em 20 de março de 2025.

**Figura 2.9, página 49:** Foto obtida de *Article for abacus, 9th edition Encyclopedia Britannica, volume 1 (1875)*, digitalizada por Malcolm Farmer e disponibilizada no endereço `https://commons.wikimedia.org/wiki/File:Abacus_6.png` Domínio público. Consultado em 17 de outubro de 2016.

**Figura 2.4, página 34:** Parte de manuscrito de Gottfried W. Leibniz alocado na Gottfried Wilhelm Leibniz Bibliothek, Hannover, e disponibilizado em `https://commons.wikimedia.org/wiki/File:Leibniz_binary_system_1697.jpg` Domínio público. Consultado em 21 de setembro de 2016.

**Figura , página 38:** Fotografia de tablete sumério depositado na *Yale Babylonian Collection's Tablet YBC 7289* `http://nelc.yale.edu/` A fotografia é de Bill Casselman `http://www.math.ubc.ca/~cass/Euclid/ybc/ybc.html` e disponibilizada em 25 de maio de 2007 no endereço `https://commons.wikimedia.org/wiki/File:Ybc7289-bw.jpg`. Permissão de uso sob os termos de *GNU Free Documentation License* `/en.wikipedia.org/wiki/GNU_Free_Documentation_License`

**Figura 2.6, página 40:** Desenho de inscrição Khmer mostrando o numeral 605. Obtido em `https://commons.wikimedia.org/wiki/File:Khmer_Numerals_-_605_from_the_Sambor_inscriptions.jpg` Disponibilizado pelo autor Paxse em 11 de janeiro de 2009 e licenciado sob licença *Creative Commons Attribution-Share Alike*. Consultado em 21 de setembro de 2016.

**Figura 2.7, página 41:** Detalhe do livro de Datta, B. e Singh, A. N. *History of Hindu mathematics, a source book*. Lahore, Motilal Banarsi Das, 1935, páginas 105 a 121. Obtido em `https://commons.wikimedia.org/wiki/File:Numeration-brahmi_fr.png` Disponibilizado por Piero em 17 de fevereiro de 2010 sob domínio público. Consultado em 21 de setembro de 2016.

**Figura 2.8, página 48:** À esquerda, foto de um ábaco escolar (Dinamarca, princípios do Séc. XX). Domínio público. Diponibilizado por Noe em `https://commons.wikimedia.org/wiki/File:Kugleramme.jpg`. À direita, foto de um ábaco russo, disponibilizado por Tor Svensson sob GNU Free Documentation License em `https://commons.wikimedia.org/wiki/File:Kulram.jpg` Consultas feitas em 21 de março de 2024.

## Capítulo 3: A arte de calcular

**Figura 3.4, página 72:** Antiga tábua de multiplicação chinesa, datada de 446-221 a.C. depositada na Tsinghua University. Disponibilizado em 13 de março de 2014 no endereço `https://commons.wikimedia.org/wiki/File:Qinghuajian,_Suan_Biao.jpg` Domínio público. Consultado em 26 de setembro de 2016.

## Capítulo 4: O ideal matemático da Antiga Grécia

**Figura 4.1, página 97:** Mapa mostrando os territórios gregos e colônias na época do Período Arcaico. Disponibilizado em 30 de março de 2014 pelo autor Regaliorum no endereço `https://commons.wikimedia.org/wiki/File:Greek_Colonization_Archaic_Period.png` Domínio público. Consultado em 4 de dezembro de 2016.

**Figura 4.2, página 101:** Recorte do quadro *Escola de Atenas*, de Rafael Sanzio, disponibilizado em `http://christusrex.org/www1/stanzas/S2-Segnatura.html` Domínio público. Consultado em 12 de março de 2002.

**Figura 4.3, página 102:** Foto de quadro de Leonard Paul Euler, do artista Jakob Emanuel Handmann (1718–1781), do Museum of Science and Technology in Munich, Alemanha. Disponibilizado em `https://commons.wikimedia.org/wiki/File:Leonhard_Euler_2.jpg` Domínio Público. Consultado em 16 de abril de 2025.

**Figura 4.4, página 105:** Digitalização da capa de uma versão de 1912 do livro Ganita Sara Sangraha, de autoria de Mahavira, traduzido do sânscrito para o inglês. Disponibilizado em `https://commons.wikimedia.`

org/wiki/File:Ganita_Sara_Sangraha_-_Sanskrit.djvu?page=1 Domínio Público. Consultado em 24 de abril de 2025.

**Figura 4.5, página 106:** Foto de estátua de Nicômaco de Gerasa, situada na cidade de Nuremberg, Alemanha. Disponibilizada por MatthiasKabel em 3 de outubro de 2010 em https://commons.wikimedia.org/wiki/File:Schoener_Brunnen_detail_blur.jpg sob *GNU Free Documentation License*. Consultado em 9 de dezembro de 2016.

**Figura 4.7, página 119:** Desenho cotado de http://www-history.mcs.st-andrews.ac.uk/Biographies/Theon_of_Smyrna.html Sem informações sobre direitos autorais. Consultado em 17 de janeiro de 2017.

**Figura 4.8, página 122:** Foto de Srinivasa Ramanujan Aiyangar. Disponibilizada em https://commons.wikimedia.org/wiki/File:Srinivasa_Ramanujan_-_OPC_-_1.jpg sob domínio público. Consultado em 26 de janeiro de 2017.

**Figura 4.9, página 123:** Foto de estátua de Aryabhata, situada no Inter-University Centre for Astronomy and Astrophysics (IUCAA), na Universidade de Pune, Índia. Disponibilizada em https://commons.wikimedia.org/wiki/File:2064_aryabhata-crp.jpg sob domínio público. Consultado em 17 de janeiro de 2017.

**Figura 4.10, página 125:** Digitalização de página de carta de 1742 de Christian Goldbach a Leonhard Paul Euler. Disponibilizada em https://commons.wikimedia.org/wiki/File:Letter_Goldbach-Euler.jpg sob domínio público. Consultado em 7 de maio de 2025.

**Figura 4.11, página 129:** Foto de pintura de autoria de Christian Albrecht Jensen retratando Johann Carl Friedrich Gauss. Disponibilizada em https://commons.wikimedia.org/wiki/File:Carl_Friedrich_Gauss_1840_by_Jensen.jpg sob domínio público. Consultado em 21 de janeiro de 2017.

## Capítulo 5: Números primos e compostos

**Figura 5.1, página 142:** Eratóstenes de Cirene. Imagem disponibilizada no endereço https://commons.wikimedia.org/wiki/File:Portrait_of_Eratosthenes.png Domínio público. Consultado em 6 de novembro de 2016.

**Figura 5.2, página 144:** Euclides de Alexandria. Imagem disponibilizada no endereço https://commons.wikimedia.org/wiki/File:Euklid-von-Alexandria_1.jpg Domínio público. Consultado em 5 de novembro de 2016.

**Figura 5.3, página 145:** Imagem de Peter G. L. Dirichlet, de autor desconhecido, disponibilizada no endereço https://commons.wikimedia.org/wiki/File:Peter_Gustav_Lejeune_Dirichlet.jpg Domínio público. Consultado em 19 de maio de 2025.

**Figura 5.4, página 148:** Digitalização da capa da primeira edição de Sir Henry Billingsley em língua inglesa de *Os Elementos* de Euclides de Alexandria, datada de 1570. Imagem disponibilizada no endereço https://commons.wikimedia.org/wiki/File:Title_page_of_Sir_Henry_Billingsley's_first_English_version_of_Euclid's_Elements,_1570_(560x900).jpg Domínio público. Consultado em 6 de novembro de 2016.

## Capítulo 7: O Teorema Fundamental da Aritmética

**Figura 7.1, página 179:** Imagem de Marin Mersenne. Disponibilizada no endereço https://commons.wikimedia.org/wiki/File:Marin_mersenne.jpg Fonte: H Loeffel. Domínio público. Consultado em 15 de junho de 2025.

**Figura 7.2, página 182:** Digitalização de páginas da tradução para o árabe das Cônicas de Apolônio feita por Thābit ibn Qurrah. Disponibilizada no endereço https://en.wikipedia.org/wiki/Thabit_ibn_Qurra#/media/File:Conica_of_Apollonius_of_Perga_fol._162b_and_164a.jpg Fonte: MartinPoulter. Licenciada sob Creative Commons Attribution 4.0 International license. Consultado em 15 de junho de 2025.

## Capítulo 8: Os ternos pitagóricos

**Figura 8.1, página 189:** Foto de monumento a Pierre de Fermat realizado por Alexandre Falguière em Beaumont-de-Lomagne Tarn-et-Garonne, France, em 1881. Disponibilizada no endereço https://commons.

wikimedia.org/wiki/File:Beaumont-de-Lomagne_-_Monument_a_Fermat.jpg Fonte: Didier Descouens. Licenciado sob Creative Commons Attribution-Share Alike 4.0 International license. Consultado em 16 de junho de 2025.

## Capítulo 9: Os números inteiros

**Figura 9.1, página 198:** Foto de Giusepe Peano, por autor desconhecido. Disponibilizada no endereço https://commons.wikimedia.org/wiki/File:Giuseppe_Peano.jpg Domínio público. Consultado em 22 de junho de 2025.

**Figura 9.2, página 209:** Digitalização da capa da 1ª. edição do livro *Disquisitiones Arithmeticae* de Johann C. F. Gauss, publicada em 1801. Disponibilizada por Lenthe no endereço https://pt.wikipedia.org/wiki/Disquisitiones_Arithmeticae#/media/Ficheiro:Disqvisitiones-800.jpg Domínio público. Consultado em 22 de junho de 2025.

## Capítulo 10: O Método da Indução Completa

**Figura 10.1, página 219:** Foto de monumento a Fibonacci, ou Leonardo de Pisa, de autoria de Giovanni Paganucci, em 1863, no Camposanto di Pisa, Itália. Licenciada por Hans-Peter Postel no endereço https://commons.wikimedia.org/wiki/File:Leonardo_da_Pisa.jpg sob Creative Commons Attribution 2.5 Generic license. Consultado em 26 de junho de 2025.

**Figura 10.2, página 223:** Foto de François E. A. Lucas, de autor desconhecido, disponibilizada no endereço https://commons.wikimedia.org/wiki/File:Elucas_1.png. Domínio público. Consultado em 27 de junho de 2025.

## Capítulo 11: A equação $ax + by = c$

**Figura 11.1, página 225:** Capa do livro *Arithmetica*, de Diofanto de Alexandria, em uma edição latina, traduzida do grego por Claude Gaspard Bachet de Méziriac. Essa edição foi publicada em 1670, e contém notas adicionais de Pierre de Fermat. O original pertence à Bibliothèque de Genève. Disponibilizada no endereço https://commons.wikimedia.org/wiki/File:Diophantus-cover-Fermat.jpg por Leonid. Domínio público. Consultado em 30 de junho de 2025.

## Capítulo 12: Aplicativos computacionais para TN

**Figura 12.1, página 231:** Foto de exemplar da calculadora Pascalina, depositada no Museu de Artes e Ofícios de Paris. Disponibilizada no endereço https://commons.wikimedia.org/wiki/File:Arts_et_Metiers_Pascaline_dsc03869.jpg por David.Monniaux. Licenciada sob GNU Free Documentation License. Consultado em 3 de junho de 2025.

**Figura 12.2, página 236:** Foto de pintura de Pacioli feita por Jacopo de Barbari, depositada no Museu de Capodimonti. Disponibilizada no endereço https://en.wikipedia.org/wiki/Luca_Pacioli#/media/File:Pacioli.jpg. Domínio público. Consultado em 12 de junho de 2025.

**Figura 12.3, página 240:** Foto de Godfrey H. Hardy, de autor desconhecido, que aparece em uma das edições de seu livro *A mathematician's apology*. Disponibilizada no endereço https://pt.wikipedia.org/wiki/Godfrey_Harold_Hardy#/media/Ficheiro:Ghhardy@72.jpg. Domínio público. Consultado em 14 de junho de 2025.

# Referências Bibliográficas


[1] Aaboe, A. *Episódios da História Antiga da Matemática.* Rio de Janeiro: Sociedade Brasileira de Matemática, 1984.

[2] Abreu, J. B. et alii. *Manual do Maxima em português.* `http://www.professores.im-uff.mat.br/hjbortol/disciplinas/2006.2/esp00000/arquivos/maxima_pt.pdf` Consultado em junho de 2025.

[3] Aczel, A. D., *Fermat's Last Theorem. Unlocking the secret of an ancient mathematical problem.* New York: Four Walls Eight Windows, 1996.

[4] Allenby, R. B. J. T. e Redfern, E. J., *Introduction to Number Theory with Computing.* London: Edward Arnold, 1989.

[5] Andrade, L. N. *Maxima: um programa para as aulas de Matemática.* João Pessoa: UFPB, 2015. `https://mat.ufpb.br/~lenimar/maxprofmat.pdf` Consultado em junho de 2025.

[6] Atkin, A. O. L. e Birch, B. J., *Computers in Number Theory.* London: Roystar Printers, 1971.

[7] Barbeau, E. J., Klamkin, S. e Moser, W. O. J., *Five Hundred Mathematical Challenges.* Washington: The Mathematical Association of America, 1995.

[8] Barnett, I. A., *Elements of Number Theory.* Boston: Prindle, Weber & Schimidt, 1969.

[9] Bezuszka, S. J. e Kenney, M. J., *Challenges for enriching the curriculum: Arithmetic and Number Theory.* Mathematics Teacher, vol. 76, nº 4, 1983.

[10] Blum, M., *Home Page.* `http://www.cs.berkeley.edu/~blum/` Consultado em 30 de maio de 2008.

[11] Bogoshi, J. *et alii, The oldest mathematical artifact.* Math. Gazette, v. 71, I. 458, 1987, pág. 294.

[12] Brandreth, G., *Number Play.* New York: Rawson Associates, 1984.

[13] Boyer, C. B., *História da Matemática.* Tradução de Gomide, E. F. São Paulo: Editora Edgard Blücher LTDA, 1974.

[14] Brutlag, D., *Making Your Own Rules.* Mathematics Teacher, vol. 83, nº 8, 1990, págs. 608 a 611.

[15] Bueno, A., *Olavo Bilac, Obra Reunida.* Rio de Janeiro: Editora Nova Aguillar, 1997.

[16] Burton, D. M., *Elementary Number Theory.* Boston: Allyn and Bacon, 1976.

[17] Caldwell, C. e Honaker, G. L., *Prime Curios!.* `http://primes.utm.edu/curios/` Consultado em 20 de janeiro de 2008.

[18] Cardoso, M. L. e Gonçalves, O. A., *Uma interpretação geométrica do* mmc. Revista do Professor de Matemática, nº 32, 3º quadrimestre de 1996, págs. 27 a 28.

[19] Carroll, L., *Alice Through the Looking Glass.* `http://www.cs.indiana.edu/metastuff/dir.html` Consultado em 20 de janeiro de 2008.

[20] Chapman, R., *A Guide to Arithmetic.* `http://www.maths.ex.ac.uk/~rjc/notes/arith.pdf` Consultado em 20 de janeiro de 2008.

[21] Chevalier, J. e Gheerbrant, A., *Dicionário de Símbolos.* Tradução de Silva, V. C., *et alii.* 12ª. edição. Rio de Janeiro: Editora José Olympio. Data da edição original: 1982.

[22] Childs, L., *A Concrete Introduction to Higher Algebra.* Springer Verlag, 1992.

[23] CONMETRO, *Resolução nº 12/88.* `http://www.inmetro.gov.br/` Consultado em 20 de janeiro de 2008.

[24] Coutinho, S. C., *Números Inteiros e Criptografia.* Série de Computação e Matemática. Rio de Janeiro: Sociedade Brasileira de Matemática e Instituto de Matemática Pura e Aplicada, 1997.

[25] Cunha, C. F., *Gramática da Língua Portuguesa.* Rio de Janeiro: Ministério da Educação, 1990.

[26] Crump, T., *The Anthropology of Numbers.* Cambridge: Cambridge University Press, 1990.

[27] Datta, B. e Singh, A. N. *History of Hindu mathematics, a source book.* Lahore: Motilal Banarsi Das, 1935.

[28] Dickson, L. E., *History of the Theory of Numbers.* New York: Chelsea Publ. Comp., 1952.

[29] Domingues, H. H., *Fundamentos de Aritmética.* São Paulo: Atual Editora, 1991.

[30] Duarte, N., *O Ensino da Matemática na educação de adultos.* São Paulo: Cortez Editora, 1986.

[31] Dumont, I., *Elementos de Aritmética.* Livraria Francisco Alves.

[32] Ebbinghaus, H.-D. *et alii*, *Numbers.* New York: Springer Verlag, 1991.

[33] Edwards, H. M., *Fermat's Last Theorem, a Genetic Introduction to Algebraic Number Theory.* New York: Springer Verlag, 1977.

[34] Eels, W. C., *Number Systems of the North American Indians.* American Mathematical Monthly, vol. XX, nº 10, 1913, págs. 293 a 299.

[35] Escultura, E., *A number trick explained with Algebra.* Mathematics Teacher, vol. 76, nº 1, 1983.

[36] Euler, L, *Elements of Algebra.* New York: Springer Verlag, 1984.

[37] Eves, H., *Introdução à História da Matemática.* Tradução de Domingues, H. H. Campinas: Editora UNICAMP, 2004.

[38] Exame Nacional de Desempenho de Estudantes (ENADE) `http://www.inep.gov.br/superior/enade/` Consultado em 04 de março de 2008.

[39] Ferreira, A. B. H., *Novo Dicionário da Língua Portuguesa.* 2ª. edição. Rio de Janeiro: Editora Nova Fronteira, 1986.

[40] Ferreira, M. K. L. (Org.), *Ideias Matemáticas de Povos Culturalmente Distintos.* São Paulo: Editora Global, 2002.

[41] Fowler, D. H. *The Mathematics of Plato's Academy. A new reconstruction.* Oxford: Clarendon Press, 1990.

[42] Fraenkel, A. S., *Systems of Numeration.* American Mathematical Monthly, vol. 92, nº 2, 1985, págs. 105 a 114.

[43] Garcia, A. e Lequain, Y. *Elementos de Álgebra.* Rio de Janeiro: IMPA, 2005.

[44] Gauss, C. F., *Disquisitiones Arithmeticae.* New York: Springer Verlag, 1986.

[45] Glaser, A., *History of Binary and Other Nondecimal Numeration.* Tomash Publishers, 1981.

[46] Graham, R. L., Knuth, D. E. e Patashnik, O., *Concrete Mathematics.* Addison-Wesley, 1990.

[47] Grosso, C., *O número 12.* Revista do Professor de Matemática, nº 67, 3º quadrimestre de 2008, págs. 14 e 15.

[48] Heath, T. L., *A Manual of Greek Mathematics.* New York: Dover Publications, 1963.

[49] Hefez, A., *Elementos de Aritmética.* Coleção Textos Universitários. Rio de Janeiro: Sociedade Brasileira de Matemática, 2005.

[50] Hefez, A., *Curso de Álgebra.* 4ª. ed. Coleção Matemática Universitária. Rio de Janeiro: IMPA, 2010.

[51] Herstein, I., *Tópicos de Álgebra.* Trad. Bergamasco, A. P. e Monteiro, L. H. J. São Paulo: EDUSP e Ed. Polígono, 1970.

[52] Honsberger, R. (ed.), *Mathematical Gems.* vol. I, II e III. Mathematical Association of America, 1973.

[53] Houaiss, *Dicionário Houaiss da Língua Portuguesa.* 1ª. edição. Rio de Janeiro: Objetiva, 2001.

[54] Ifrah, G., *Os Números, história de uma grande invenção.* Tradução de Senra, S. M. F. 3ª. edição. São Paulo: Editora Globo, 1989.

[55] Ignatiev, E. J., *En el Reino del Ingenio.* Moscou: Editorial Mir, 1986.

[56] Kamii, C. e DeClark, G., *Reinventando a Aritmética (implicações da Teoria de Piaget).* Tradução de Curt, E. *et alii.* Campinas: Papirus Editora, 1994.

[57] Kamii, C. e Joseph, L. L., *Aritmética, Novas Perspectivas.* Tradução de Lellis, M. C. T. *et alii.* Campinas: Papirus Editora, 1995.

[58] Kamii, C., *A Criança e o Número.* Tradução de Assis, R. A. 39ª edição. Campinas: Papirus Editora, 1995.

[59] Karpinski, L. C., *The History of Mathematics.* New York: Russel & Russel, 1965.

[60] Kato, K., Kurokawa, N. e Saito, T., *Number Theory 1, Fermat's Dream.* Providence, Rhode Island: American Mathematical Society, 2000.

[61] Kirch, A. M., *Elementary Number Theory: a Computer Approach.* New York: Intext Educational Publishers, 1974.

[62] Lang, S., *Undergraduate Algebra.* New York: Springer Verlag, 1987.

[63] LeVeque, W. J., *Fundamentals of Number Theory.* Reading, Massachusetts: Addison-Wesley, 1977.

[64] Liwer, A., *Don't regroup.* Arithmetic Teacher, Reston, vol. 37, nº 7, pág. 2, março de 1990.

[65] Long, C. T., *Elementary Introduction to Number Theory.* Englewood Cliffs: Prentice-Hall, 1987.

[66] Lopes, J. J., *Vejam o que o Adriano aprontou!* Revista do Professor de Matemática, nº 18, 1º semestre de 1991, págs. 21 a 23.

[67] Lorenzato, S., *Educação infantil e percepção matemática.* Campinas: Editores Associados, 2006.

[68] Lovász, L., Pelikán, J. e Vesztergombi, K., *Matemática Discreta.* Coleção Textos Universitários. Rio de Janeiro, Sociedade Brasileira de Matemática, 2006.

[69] Lucas, *Evangelho segundo São Lucas. in* Bíblia Sagrada. São Paulo, Editora Ave Maria, 1991.

[70] Mandarino, M. C. F. e Belfort, E., *Números Naturais - Conteúdo e Forma.* Matemática nas Séries Iniciais - Parte I. Rio de Janeiro: Laboratório de Pesquisa e Desenvolvimento em Ensino de Matemática e das Ciências, UFRJ, 2005.

[71] Martinez, F. B. *et alii. Teoria dos Números.* Rio de Janeiro: Sociedade Brasileira de Matemática, 2024.

[72] Massago, S. *Tutorial de Maxima no formato WxMaxima.* `https://www.dm.ufscar.br/profs/sadao/maxima/index.php` Consultado em junho de 2025.

[73] *Mathematics.* `http://math.stackexchange.com/` Consultado em novembro de 2016.

[74] Mathematics Teacher. Reston, National Council of Teachers of Mathematics. Seção *Calendar Problems* de vários fascículos.

[75] *Maxima.* `http://maxima.sourceforge.net` *Maxima Manual.* Versão 5.17.1. `https://maths.cnam.fr/Membres/wilk/MathMax/help/Maxima/maxima.html` Consultado em junho de 2025.

[76] Mega, E. e Watanabe, R., *Olimpíadas Brasileiras de Matemática 1ª a 8ª.* São Paulo: Editora Núcleo e Sociedade Brasileira de Matemática, 1988.

[77] Merrill, H. A., *Mathematical Excursions.* New York: Dover Publications, 1933.

[78] MIT, *Problems on congruences and divisibility.* 2002. `http://ocw.mit.edu/OcwWeb/Mathematics/18-S34Fall-2004/DownloadthisCourse/index.htm` Consultado em 20 de janeiro de 2008.

[79] Moise, E. E., *The Number Systems of Elementary Mathematics.* Reading, Massachusetts: Addison-Wesley Publishing Company, 1966.

[80] Monteiro, L. H. J., *Elementos de Álgebra.* Coleção Elementos de Matemática. Rio de Janeiro: Instituto de Matemática Pura e Aplicada, Universidade de São Paulo e Ao Livro Técnico, 1969.

[81] Nacarato, A. M., *A matemática nos anos iniciais do ensino fundamental.* Belo Horizonte: Autêntica Editora, 2009.

[82] Nery, C. e Possani, C., *Os Primos Esquecidos.* Revista do Professor de Matemática, nº 47, 3º quadrimestre de 2001, págs. 16 a 20.

[83] Nery, C., *Ensino, logo aprendo.* Revista do Professor de Matemática, nº70, 3ºquadrimestre de 2009, págs. 17 a 22.

[84] Neugebauer, O. E. e Sachs, A. J., (eds) *Mathematical Cuneiforms Texts.* New Haven: American Oriental Society, 1946, American Oriental Series, vol. 29.

[85] Neugebauer, O. E., *The Exact Sciences in Antiquity.* Princeton: Princeton University Press, 1952; 2nd edition, Brown University Press, 1957; reprint, New York: Dover publications.

[86] Nicolai, R., *Algumas técnicas operatórias.* Revista do Professor de Matemática, nº8, 1ºsemestre de 1986, págs. 42 a 45.

[87] O'Connor, J. J. e Robertson, E. F. *A history of Zero.* `http://www-history.mcs.st-and.ac.uk/history/HistTopics/Zero.html` Consultado em 8 de dezembro de 2016.

[88] Ogilvy, C. S. e Anderson, J. T., *Excursions in Number Theory.* Englewood Cliffs: Prentice-Hall, 1987. New York: Oxford University Press, 1966.

[89] OBMEP. *Provas das Olimpíadas Brasileiras de Matemática das Escolas Públicas.* `http://www.obmep.org.br/provas.htm` Consultado em 04 de março de 2008 e em 24 de março de 2025.

[90] Oliveira, Z. C., *Uma interpretação geométrica do* mdc. Revista do Professor de Matemática, nº 29, 3º quadrimestre de 1995, págs. 24 a 26.

[91] Ore, O., *Invitation to Number Theory.* New York: Random House, 1967.

[92] Paterlini, R. R., *O ensino da Aritmética em cursos de Licenciatura em Matemática.* `http://www2.dm.ufscar.br/Hp_2001/hp591/hp591001/hp591001.html` Consultado em 20 de janeiro de 2008.

[93] Paterlini, R. R., *O que é o Método Genético para o ensino da Matemática.* `http://www2.dm.ufscar.br/Hp_2001/hp400/hp400.html` Consultado em 20 de janeiro de 2008.

[94] Paterlini, R. R. *Aritmética dos números reais.* São Carlos, UFSCar, 2008. `http://www.dm.ufscar.br/~ptlini/livros/` Consultado em 20 de janeiro de 2008.

[95] Polezzi, M., *Como obter o MDC e o MMC sem fazer contas?* Revista do Professor de Matemática, nº51, 2ºquadrimestre de 2003, págs. 29 a 31.

[96] Pedoe, D., *The Gentle Art of Mathematics.* New York: Dover Publications, 1958.

[97] Pereira, A. L. e Watanabe, R., *Leitura de números grandes.* Revista do Professor de Matemática, nº57, 2ºquadrimestre de 2005, pág. 59.

[98] Pérez, J. A. S., *La Aritmetica en Roma en India y en Arabia.* Madrid: Instituto Miguel Asín, 1949.

[99] Piaget, e Szeminska, A., *A Gênese do Número na Criança.* Tradução de Oiticica, C. M. Segunda edição. Rio de Janeiro: Zahar Editores, 1975.

[100] Pisa, Programa Internacional de Avaliação de Alunos. `http://www.inep.gov.br/internacional/pisa/Novo/oquee.htm` Consultado em 20 de janeiro de 2008.

[101] Revista do Professor de Matemática. São Paulo: Sociedade Brasileira de Matemática. Seção *Problemas* de diversos números. Seção *Cartas* de diversos números.

[102] Ribenboim, P., *Números Primos: mistérios e recordes.* Coleção Matemática Universitária. Rio de Janeiro: Instituto de Matemática Pura e Aplicada, 2001.

[103] Robertson, J. I., *How to do Arithmetic.* American Mathematical Monthly, nº86, 1979, págs. 431 a 439.

[104] Rosen, K. H., *Elementary Number Theory and its Applications.* Reading, Massachusetts: Addison-Wesley Publishing Company, 1984.

[105] Rothbart, A. e Paulsell, B., *Números Pitagóricos: uma fórmula de fácil dedução e algumas aplicações geométricas.* Revista do Professor de Matemática, nº7, 1ºsemestre de 1985, págs. 49 a 51.

[106] Roxo, E., *Lições de Arithmetica.* Livraria Francisco Alves, 1926.

[107] Santos, A. L., Wagner, E. e Agostino, R. F. W., *Olimpíadas de Matemática do Estado do Rio de Janeiro.* São Paulo, Atual Editora e Sociedade Brasileira de Matemática, 1995.

[108] Santos, J. P. O., *Introdução à Teoria dos Números.* Coleção Matemática Universitária, Rio de Janeiro, Instituto de Matemática Pura e Aplicada, CNPq, 1998.

[109] Shakespeare, W., *Taming of the Shrew.* `http://www.shakespeare-literature.com/` Consultado em 20 de janeiro de 2008..

[110] Shoemaker, R. W., *Patterns in Powers of Digits.* Mathematics Teacher, vol. 81, nº 4, 1988.

[111] Sierpinski, W., *250 Problems in Elementary Number Theory.* New York: American Elsevier Publishing Company, 1970.

[112] Sloane, N. J. A. *The On-Line Encyclopedia of Integer Sequences.* `https://oeis.org/` Consultado em abril de 2025.

[113] Smith, D. E., *History of Mathematics.* volumes I e II. New York: Dover Publications, 1958.

[114] Struik, D. J., *A Concise History of Mathematics.* 3ª. edição. New York: Dover Publications, 1967.

[115] Tao, T., *Como Resolver Problemas Matemáticos.* Rio de Janeiro: Sociedade Brasileira de Matemática, 2013.

[116] Thiré, C., *Questões de Arithmetica.* Rio de Janeiro: Pimenta de Melo, 1925.

[117] Toeplitz, O., *The Calculus, a Genetic Approach.* Chicago: The University Press, 1963.

[118] Vianna, J. J. L. *Elementos de Arithmetica.* Livraria Francisco Alves, 1914. `https://pt.wikisource.org/wiki/Elementos_de_Arithmetica/Capítulo_1`

[119] Vinogradov, I. M., *Elements of Number Theory.* New York: Dover Publications, 1954.

[120] Zazkis, R. e Campbell, S. R. (ed.), *Number Theory in Mathematics Education.* New Jersey: Lawrence Erlbaum Associates, 2006.

[121] Zunino, D. L., *A Matemática na Escola: Aqui e Agora.* Tradução de Llorens, J. A. Porto Alegre: Artmed Editora, 1995.

[122] Waerden, B. L. van der, *Geometry and Algebra in Ancient Civilizations.* Berlin: Springer Verlag, 1983.

[123] Wagner, E., *Paridade.* Cubo Matemática Educacional, vol. 1, junho 1999, págs. 10 a 15.

[124] Walle, J. A. Van de, *Matemática no Ensino Fundamental.* Tradução de Colonese, P. H. Porto Alegre: Artmed Editora, 2009.

[125] Weisstein, Eric W. *MathWorld–A Wolfram Web Resource.* Item consultado: *Partition Function P;* Endereço geral: `https://mathworld.wolfram.com/` Consulta no período 2016-2025.

[126] Weil, A., *Number Theory for Beginners.* Berlim: Springer Verlag, 1979.

[127] Weil, A., *Number Theory An approach through history from Hammurapi to Legendre.* Berlim: Springer Verlag, 1979.

[128] Wikipedia. Informações e figuras. Itens consultados: *Abacus; Adelard of Bath; Amicable numbers; Aristoxenus of Cyrene; Axiomas de Peano; Blaise Pascal; Categoria:Sistemas de numeração; Christian Goldbach; Diofanto de Alexandria; Disquisitiones Arithmeticae; Édouard Lucas; Ganita-sāra-saṅgraha; Giuseppe Peano; Godfrey Harold Hardy; Goldbach's conjecture; Greek numerals; Hebrew numerals; Integer partition; Leonardo Fibonacci; Leonhard Euler; Luca Pacioli; Mahāvīra (mathematician); Maple; Marin Mersenne; Mathematica; Máxima (software); Pascalina; Peter Gustav Lejeune Dirichlet; Pierre de Fermat; Pythagoras; Rhind Mathematical Papyrus; SageMath; Sequência de Fibonacci; Sistema algébrico computacional; Thābit ibn Qurra; Twin prime.* Endereço geral: `https://en.wikipedia.org/wiki/` Consultas no período 2016-2025.

[129] Wolf, A. P., *Meus Problemas.* São Paulo: Editora Saraiva, 1947.

# Índice de nomes próprios


Adelardo de Bath (c. 1075-1160), 40
África, 10
Ahmes, c. 1650 a.C., 12
al-Khowarizmi (c. 825), 40
Alcuin de York (735-804), 229
Alexandria, 97, 142, 183
Angkor, 40
Antiga Grécia, 97, 119, 144, 225
Antropologia, 8
Apolônio de Perga (262-194 a.C.), 182, 261
Aramaico, 17
Aristoxenus (Século IV a.C.), 97
Aryabhata (c. 475-550), 123, 261
Austrália, 8

Bachet, C. G. M, (1581,1638), 228, 262
Bagdá, 40
Bhaskara (1114-1185), 58, 73, 104
Bilac, O. B. M. G. (1865-1918), 41
Bovelles, C. (1475-1566), 239
Brahmagupta (598-670), 104

Camboja, 40
Cantor, G. (1845-1918), 34
Carrol, L. (1832-1898), 3
Checoslováquia, 7
Ciência da Computação, 34, 37
CONMETRO, 45
Creta, 6

De Moivre, A. (1667-1754), 222
Descartes, R. (1596-1650), 189
Diofanto (c. 250), 189, 225, 262
Dirichlet, P. G. L. (1805-1859), 144, 145, 261

Edwards, H. M. (1936-2020), viii
Eels, W. C., 10
Epistemologia Genética, 5, 19
Eratóstenes (c. 230 a.C.), 140, 142, 261
Escola
    Alexandria, 13, 142, 144, 225
    Pitagórica, 97, 101, 106, 115, 119, 154, 178, 180, 184, 216
    Platônica, 97, 184
Espanha, 40
Etnologia, 8
Euclides (c. 300 a.C.), 97, 144, 145, 147, 179, 183, 185, 236, 261
Euler, L. P. (1707-1783), 102, 179, 189, 190, 211, 227, 229, 235, 260, 261
Europa, 14, 40

Fermat, P. (1601?-1665), viii, 37, 160, 189, 203, 209, 211, 221, 223, 261, 262
Fibonacci, ou Leonardo de Pisa (1170-1250), 40, 218, 219, 222, 223, 234, 235, 262

Gauss, J. C. F. (1777-1855), 129, 206, 209, 261, 262
Gillies, D. B. (1928-1975), 35
Goldbach, C. (1690-1764), 125, 261
Grave, D. A. (1863-1939), 212

Hardy, G. H. (1877-1947), 239, 240, 262
Heath, T. L. (1861-1940), 101
Helfgott, H. A. (1977, ...), 250
Hermite, C. (1822-1901), 145
Heron de Alexandria (10-80), 190
Hindus, 225, 227
Hipacia de Alexandria (c. 350 - 415), 13
Hiparcos (c. 190 - c. 120 a.C.), 13
Horácio Flaco (65-08 a.C.), 106

Ilhas Murray, 8, 10, 17
Índia, 123, 186, 221, 261

Jensen, C. A. (1792–1870), 261

Kamiraloi, 9, 17
Korselt, A. R. (1864-1947), 181
Kronecker, L. (1823-1891), 188
Kummer, E. E. (1810-1893), 145

Lévy-Brühl (1857-1939), 10
Leibniz, G. W. (1646-1716), 34, 212, 231, 260
LIBRAS, 6, 20
Linguagem Brasileira de Sinais, 6, 20
Lucas, F. E. A. (1842-1891), 220–223, 262

Madagáscar, 22, 24
Mahavira (c. 800-870), 104, 105, 260
Maia, 39
Maurolico, F. (1494-1575), 216
Mersenne, M. (1558-1648), 35
Mersenne, M. (1588-1648), 159, 179, 261
Mesopotâmia, 37

Neugebauer, O. E. (1899 - 1990), 259

Newton, I. (1643-1727), 151
Nicômaco (c. 100), 106, 128, 179, 251, 261
Nova Guiné, 8, 10

Os Elementos, 97, 147, 179, 185

Pacioli, L. (1445-1517), 76
Pacioli, L. B. (c. 1447-1517), 236, 262
Paraguai, 10
Pascal, B. (1623-1662), 216, 231, 262
Peano, G. (1858-1932), 198, 262
Piaget, J. (1896-1980), 5, 18
Pitágoras (c. 585-500 a.C.), 97, 101, 113, 183, 184
Platão (c. 428-348 a.C.), 119, 177
Proclus (410-485), 97, 184, 216
Ptolomeu, C. (c. 100 - c. 170), 13

Qurrah, T. (c. 826-901), 181, 182, 261

Ramanujan, S. A. (1887-1920), 122, 129, 239, 240, 261
Recorde, R. (c. 1510-1558), 57
Rhind, A. H. (1833–1863), 12, 259
Rio Murray, 17

Sanzio, R. (1483-1520), 101, 260
Sarrus, P. F. (1798-1861), 255
Shakespeare, W. (1564-1616), 3
Siríaco, 17
Sistema Internacional de Pesos e Medidas (SI), 45
Stein, W. A. (1974-), 232
Sumérios, 183

Theon de Alexandria (c. 335 - c. 405), 13
Theon de Smyrna (c. 70-135), 119
Toeplitz, O. (1881-1940), viii

UFSCar, vii, viii, 2, 109

Wiles, A. (1953 -), 189
Wolfram, S. (1958-), 232

Zermelo, E. F. F. (1871-1953), 181

# Índice de assuntos


$(d_n d_{n-1} \ldots d_2 d_1 d_0)_\beta$, 31
$(d_n d_{n-1} \ldots d_2 d_1 d_0)_{dez}$, 28
$+$, 4
$0^0$, 104
$<$, $>$, 66
$=$, 66
$[x]$, 155, 251
$\div$, 83
$\leq$, $\geq$, 66
$\lfloor x \rfloor$, 162
$\mathbb{N}$, 104
$\mathbb{N}^*$, 104
$\mathbb{Z}_+$, 194
$\mathbb{Z}_-$, 194
$\sigma$, 175
$\tau$, 175
$\times$, $\cdot$, 68
$\{a \mid c\}$ (conjunto dos elementos $a$ que cumprem a condição $c$), 201
$\{\,\}$, conjunto, 104
$a^n$, 83
$a^{m^n}$, 84
$a^{m^n}$ convenção, 84
$b \mid a$ ($b$ divide $a$), 200
$b \nmid a$ ($b$ não divide $a$), 129, 200
$\mathcal{D}(n)$, 131, 200
$\mathcal{M}(a)$, 148

ábaco, 22, 24, 48
adição, 51, 194
    ábaco, 54
    algoritmos, 53
    associativa, 52
    cálculo aproximado, 56
    comutativa, 52
    conceito, 52
    efetuar, 53
    nomenclatura, 53
    reserva, 55
    sistema hieroglífico egípcio, 53
    sistema romano, 54
    sistemas posicionais, 56
    soma ou total, 53
    técnica mental, 56
    termo ou parcela, 53
algarismos, 11
    decimais, 26
    hindu-arábicos, 26
algoritmo euclidiano, 147
aplicativos computacionais algébricos, 231
Aritmética, 97
    gênese da, 97, 113
Arte de Contar, 3
axiomas de Peano, 198

balança de dois pratos sem escala, 90

classes de restos de dois, 106
classes de restos de três, 109
classes módulo
    cinco, 113
    dois, 106
    n, 110, 207
    quatro, 110, 113
    três, 109, 112
combinação linear, 114
compatibilidade
    inteiros, 197
congruências, 206
    notação de Gauss, 206
    propriedades, 207
    resíduos, 206
conjunto
    limitado inferiormente, 198
    limitado superiormente, 198
    mínimo, 198
    máximo, 198
contar, 5
coprimos, 146, 202
critério de divisibilidade
    por cinco, 119
    por dez, 119
    por dois, 108
    por nove, 151
    por onze, 153
    por quatro, 119
    por seis, 120
    por sete, 119
    por três, 151
crivo de Eratóstenes, 138, 140
cuneiforme, 37

decomposição canônica, 115, 173
decomposição em fatores primos, 115
dedução, 97, 98

definição por recorrência, 100, 103
diferença, 195
dígitos, 28, 31
distributiva
  adição, 69
  subtração, 74
divide, 114, 200
divisível, 114
divisão, 76, 194
  algoritmos, 78
  conceito, 76
  dispositivo longo, 80
  método egípcio, 81
  nomenclatura, 79
  quociente e resto, 77
  sistemas posicionais, 81
divisor, 114, 200

ensino da Matemática
  através de problemas, vii
  método genético, viii
equação diofantina linear, 225, 227, 230

fator, 114, 200
fatoração
  canônica, 115
  em fatores primos, 115
  método de Fermat, 160
fatorial de um número, 34, 125
função $\varphi$ de Euler, 235

gnômon, 100, 184

IA, 240
identidades algébricas, 150
indução, 98

kuttaka, 225, 227

Lei da Tricotomia, 66, 197
Lei de Integridade, 104, 197
Leis de cancelamento
  adição, 60
  inteiros, 197
  multiplicação, 69, 105
  ordem/adição, 67
  ordem/subtração, 67
  subtração, 60
limitante inferior, 198
limitante superior, 198
linguagem
  de sinais, 3, 6
  de sinalização marítima, 6
  pictográfica, 3, 6, 15
  simbólica, 3, 6

maior número natural $\lfloor x \rfloor$, 162
Maxima
  descrição, 232
  exemplos, 232, 235
  lista de comandos, 234
  pequenos programas, 236
máximo divisor comum, 145, 200
Método da Indução Completa, 211
mínimo múltiplo comum, 147, 148, 201
multiplicação, 68, 194
  algoritmos, 70
  associatividade, 69
  cancelamento/ordem, 69
  compatibilidade/ordem, 69, 105
  comutatividade, 69
  conceito, 68
  distributiva/adição, 69
  distributiva/subtração, 74
  método camponês, 75
  método egípcio, 72
  método longo, 71
  métodos hindus, 73
  nomenclatura, 71
  sistemas posicionais, 72
múltiplo, 114, 200

numeral, 6
  cardinal, 6, 41
  classificação, 41
  fracionário, 44
  multiplicativo, 44
  ordinal, 6, 43
número
  automórfico, 30
  binomial, 151
  capicua, 30, 93
  cinco, 4
  composto, 113, 114, 202
  cúbico, 112
  decomposição canônica, 115, 173
  decomposição em fatores primos, 115
  dois, 4
  hexagonal, 101
  ímpar, 106
  inteiro, 193, 194
  legislação, 45
  natural, 3, 51, 104, 131
  negativo, 193, 194
  oblongo, 102
  oposto, 194
  palíndromo, 30, 93
  par, 106
  pentagonal, 101, 102, 236
  planar, 99, 113
  poliedral, 101
  positivo, 104, 194
  primo, 113, 114, 202
  quadrado, 100–102
  quatro, 4
  retilíneo, 113
  reverso, 28
  sólido, 99

três, 4
triangular, 100–102, 129
um, 4
unidade, 4
zero, 103
número natural, 3
antecessor, 4
conceito, 4
conjunto, 5
gênese, 4
igual, 66
maior do que, 66
menor do que, 66
ordem, 4, 66
sucessor, 4
números
de Fermat, 37, 211, 212, 223
de Mersenne, 35, 159
e geometria, 99
números negativos, 193

ordem, 195
cancelamento/adição, 67
cancelamento/multiplicação, 69
cancelamento/subtração, 67
compatibilidade/adição, 67
compatibilidade/subtração, 67
Lei da Tricotomia, 66
número natural, 66
transitiva, 66

paridade
mesma, 107
oposta, 107
partição aditiva, 121
Pequeno Teorema de Fermat, 203, 221
potenciação, 83
conceito, 83
convenção, 84
nomenclatura, 83
propriedades, 84, 85
primaridade, 116, 154
teste de, 118, 137, 139, 155, 158, 159, 167, 178
Primeiro Princípio da Indução Completa, 217
primo
de Euclides, 145
definição, 114, 202
primos
gêmeos, 120, 128, 136
infinitude, 115, 119, 143, 154
lista, 116, 140, 154, 243
trigêmeos, 120
primos entre si, 146, 202
Princípio
Indução, 198, 218
Menor Número Natural, 66, 198
propriedade
associativa, 104, 195
comutativa, 52, 104, 195
distributiva, 104, 195
transitiva, 197
pulverização, 227, 229

quadrado perfeito, 108

relativamente primos, 146, 202

Segundo Princípio da Indução Completa, 218
sequência de Fibonacci, 218, 234, 235
sistema de numeração
aditivo, 10
aditivo base dois, 9
aditivo base três, 9
aditivo base um, 7
alfabético, 13
ático ou herodiânico, 12
base cem, 37
base qualquer, 30
base quatro, 31
base sessenta, 32, 37
binário, 21
Cantor, 34
decimal, 3, 39
definição, 5
demótico, 12
duodecimal, 32
fatorial, 34
hierático, 12
hieroglífico egípcio, 11
hindu, 22, 39
indígenas, 8
jônico, 13
maia, 39
minóico, 15
mudança de base, 32
posicional, 21
primitivo, 7, 8
romano, 14
siríaco, 17
ternário, 127
sistema decimal
construção, 24
definição, 26
representação compacta, 27
representação expandida, 28
subtração, 59, 194
ábaco, 61, 65
algoritmos, 61
compatibilidade/ordem, 67
compensação, 62
complementação, 63
conceito, 59
diferença, 60
método austríaco, 63
nomenclatura, 63
sistema romano, 65
sistemas posicionais, 64

Teorema
    Último, de Fermat, 189
    da existência e unicidade em sistemas posicionais, 164
    de Pitágoras, 183
    do algoritmo da divisão, 161, 199
    Fundamental da Aritmética, 172
terno pitagórico, 183
    caracterização, 185, 187
    primitivo, 187
Torre de Hanoi, 221

unidade
    conceito, 4
    símbolo, 4

valor absoluto, 195
verificação
    de cálculos aritméticos, 85
    prova do nove, 85
    prova real, 85