# Fundamentos de Matemática I

Neri Terezinha Both Carvalho
Carmem Suzane Comitre Gimenez

2ª Edição
Florianópolis, 2009


## Governo Federal

**Presidente da República:** Luiz Inácio Lula da Silva
**Ministro de Educação:** Fernando Haddad
**Secretário de Ensino a Distância:** Carlos Eduardo Bielschowky
**Coordenador Nacional da Universidade Aberta do Brasil:** Celso Costa

## Universidade Federal de Santa Catarina

**Reitor:** Alvaro Toubes Prata
**Vice-Reitor:** Carlos Alberto Justo da Silva
**Secretário de Educação a Distância:** Cícero Barbosa
**Pró-Reitora de Ensino de Graduação:** Yara Maria Rauh Müller
**Pró-Reitora de Pesquisa e Extensão**: Débora Peres Menezes
**Pró-Reitor de Pós-Graduação:** Maria Lúcia de Barros Camargo
**Pró-Reitor de Desenvolvimento Humano e Social:** Luiz Henrique Vieira Silva
**Pró-Reitor de Infra-Estrutura:** João Batista Furtuoso
**Pró-Reitor de Assuntos Estudantis:** Cláudio José Amante
**Centro de Ciências da Educação:** Wilson Schmidt
**Centro de Ciências Físicas e Matemáticas:** Tarciso Antônio Grandi
**Centro de Filosofia e Ciências Humanas:** Roselane Neckel

## Cursos de Licenciaturas na Modalidade à Distância

**Coordenação Acadêmica Matemática:** Neri Terezinha Both Carvalho
**Coordenação de Ambientes Virtuais:** Nereu Estanislau Burin
**Coordenação de Infra-Estrutura e Pólos**: Vladimir Arthur Fey

## Comissão Editorial

## Laboratório de Novas Tecnologias – LANTEC/CED

### Coordenação Pedagógica

**Coordenação Geral:** Andrea Lapa

**Coordenação Pedagógica:** Roseli Zen Cerny

**Núcleo de Formação**: Nilza Godoy Gomes

**Núcleo de Pesquisa e Avaliação:** Claudia Regina Flores

### Núcleo de Criação e Desenvolvimento de Materiais

### Design Gráfico

**Coordenação:** Laura Martins Rodrigues, Thiago Rocha Oliveira

**Projeto Gráfico Original:** Diogo Henrique Ropelato, Marta Cristina Goulart Braga, Natal Anacleto Chicca Junior.

**Redesenho do Projeto Gráfico:** Laura Martins Rodrigues, Thiago Rocha Oliveira

**Diagramação:** Gabriel Nietsche

**Ilustrações:** Pricila Cristina da Silva, Gabriel Nietsche

**Capa:** Thiago Felipe Victorino

### Design Instrucional

**Coordenação:** Juliana Machado

**Design Instrucional:** Janice Pereira Lopes

**Revisão do Design Instrucional:** Márcia Maria Bernal

**Revisão Gramatical:** Jane Maria Viana Cardoso



## Ficha Catalográfica

C331f Carvalho, Neri Terezinha Both
Fundamentos de matemática I / Neri Terezinha Both Carvalho, Carmen Suzane Comitre Gimenez. – 2. ed. – Florianópolis : UFSC/EAD/CED/CFM, 2009.
207 p.

ISBN 978-85-99379-73-8

1. Matemática. I. Gimenez, Carmem S. Comitre. II. Título.
CDU 51

**Elaborada pela Bibliotecária Eleonora M. F. Vieira – CRB – 14/786**

# Sumário

# Apresentação

A matemática, como a língua materna, é considerada básica para o exercício pleno da cidadania e para a compreensão das outras áreas do conhecimento e leitura do mundo.

A matemática, no contexto dos conjuntos numéricos, constitui um conjunto organizado, sistematizado e possui uma representação simbólica definida e universal.

Tratamos, neste livro, dos conjuntos numéricos: naturais, inteiros e racionais enquanto objetos do conhecimento matemático, os quais são estruturados de maneira lógica e expressos por uma simbologia própria.

Por que estudar os conjuntos numéricos?

Podemos pensar que os conjuntos numéricos compõem o passo inicial da representação, da expressão de informações, além de sua importância no fazer matemática; eles são considerados essenciais para a vida do cidadão na sociedade atual. É praticamente impossível a prática da vida no dia-a-dia sem o conhecimento dos números.

Você já se imaginou passar um dia, sem usar em algum momento uma informação que envolva números? Quantidade, valor, hora etc.

Este livro tem por objetivo apresentar as operações e propriedades dos conjuntos numéricos $\mathbb{N}$, $\mathbb{Z}$ e $\mathbb{Q}$; elementos da história dos números; bases e sistemas de numeração; o conceito de divisibilidade e critérios de divisibilidade; princípios de indução; congruência; Teorema fundamental da Aritmética; Algoritmo da divisão. Enfim, vamos trabalhar a estrutura dos conjuntos numéricos do ponto de vista da teoria dos números.

O livro está organizado em seis capítulos. No primeiro capítulo, estudaremos Elementos de História dos Números e Sistemas de Numeração em Diferentes Bases. Neste capítulo abordamos algumas informações históricas, situamos a problemática propul-

sora da formulação dos sistemas de numeração e sua evolução até a concepção e estabelecimento do sistema de numeração decimal como universal.

No segundo capítulo, apresentaremos os conjuntos numéricos Naturais e Inteiros. Introduzimos os conjuntos numéricos $\mathbb{N}$ e $\mathbb{Z}$, apresentando seus elementos, as operações definidas em cada conjunto com suas respectivas propriedades. Fazemos uma apresentação da estrutura de cada um dos conjuntos numéricos, naturais e inteiros, de maneira sistemática.

Desenvolvemos o Algoritmo da divisão em $\mathbb{Z}$ e o conceito de divisibilidade no terceiro capítulo. Também neste capítulo exploramos as conseqüências do conceito de divisibilidade com estudo do máximo divisor comum, mínimo múltiplo comum, equações diofantinas e congruências. Esta parte do conteúdo fornece um instrumental importante para a resolução de exercícios. Neste capítulo o conjunto de exercícios propostos é variado e abundante.

O quarto capítulo é dedicado ao Teorema Fundamental da Aritmética, que envolve o estudo de números primos e aplicações da fatoração.

O quinto capítulo apresenta o Princípio da Indução finita, um procedimento para demonstrações de certos tipos de resultados.

Finalizamos com o estudo do conjunto dos números racionais no sexto capítulo.

*Neri Terezinha Both Carvalho*

*Carmem Suzane Comitre Gimenez*

# Capítulo 1

## Elementos da História dos Números e Sistemas de Numeração em Diferentes Bases

# Capítulo 1

## Elementos da História dos Números e Sistemas de Numeração em Diferentes Bases

*Neste capítulo estudaremos o sistema de numeração na base dez e a lei de formação dos números de um sistema de numeração em uma base qualquer.*

*Este capítulo tem, ainda, o objetivo de apresentar alguns elementos da história relativos aos sistemas de numeração e desenvolver um estudo que oferece ao leitor a compreensão do funcionamento de um sistema de numeração posicional independentemente da base considerada.*

## 1.1 Elementos da história

A numeração escrita é muito antiga. A evolução da numeração encontra sua expressão final no sistema de numeração decimal.

Cálculos que atualmente uma criança realiza, exigiam, na antiguidade, os serviços de um especialista. As dificuldades experimentadas, na época, eram inerentes ao sistema de numeração em uso, os quais não eram suscetíveis a regras simples e diretas. Nenhum sistema da antiguidade era capaz de criar uma aritmética que pudesse ser utilizada por um homem de inteligência média. Por isso, até o advento do sistema de *numeração posicional*, foram feitos poucos progressos na arte de calcular.

Conhecer um pouco da história da evolução dos conhecimentos facilita, muitas vezes, a compreensão sobre o que se usa, o que se explora, ao que damos maior ênfase, no presente. Conhecer a evolução permite compreender as modificações que sofreram os sa-

beres ao longo da história. O que estudamos, no presente, são os resultados de um estágio da evolução. Existe um movimento científico paralelo ao movimento cultural e de desenvolvimento dos povos.

### 1.1.1 Contagem: a idéia da correspondência, os sistemas de numeração e estruturas

Os mais antigos documentos escritos de que dispomos mostram a presença do conceito de "número"; todos contêm a questão: "Quantos?" Estes documentos provém da China, Índia, Egito e Mesopotâmia e têm aproximadamente 6000 anos. Provavelmente, muito antes desta época, o conceito de número como forma de contagem já existia: uma tíbia de lobo com 55 cortes transversais divididos em blocos de 5 foi encontrada na Tchecoslováquia e data de aproximadamente 30 000 a.C.

As primeiras culturas a usar símbolos especiais para os números desenvolveram-se junto a grandes rios: China, norte da Índia, Egito e Mesopotâmia. Aparentemente, tudo começou com a idéia de "correspondência": é comum a história do pastor que, para saber se não faltava nenhuma ovelha na hora de recolher o rebanho, fazia uma correspondência das ovelhas com um conjunto de pedrinhas; cada ovelha que entrava, uma pedrinha era separada. Se sobrassem pedrinhas, faltavam ovelhas. É claro que este pastor fez uma "correspondência inicial", ou seja, seu conjunto de pedrinhas correspondia ao seu conjunto de ovelhas. Esta idéia de "conjunto" foi uma das primeiras abstrações feitas pelo homem e a correspondência entre conjuntos foi o primeiro passo para a contagem.

Os primeiros tipos de correspondência usavam o corpo humano: dedos das mãos, dos pés, pulso, cotovelo, ombro etc., numa certa ordem. Algumas civilizações chegavam até o 31, usando todos os dedos das mãos e dos pés e mais onze partes do corpo; algumas chegavam a 100. De início, não havia palavras específicas para números, nem o conceito de número de forma abstrata; o surgimento de palavras-número não implica, por si só, o aparecimento do conceito de número, mas, sem dúvida levou a ele. Resumindo, isto parece ter ocorrido da seguinte forma:

a) aparecimento da idéia de "conjunto" e correspondência entre conjuntos;

b) a ordem dos objetos que se desejava contar era irrelevante (era indiferente começar a contagem pelas ovelhas pretas ou brancas);

c) conjuntos de objetos distintos poderiam ser postos em correspondência com o "*mesmo*" conjunto (de pedrinhas ou partes do corpo humano). Este passo foi decisivo; em termos de símbolos, o mesmo símbolo poderia ser usado para indicar 10 ovelhas ou 10 ânforas de vinho;

d) o nome do último número enunciado não só atribuía um nome ao último objeto do conjunto a ser contado como, também, dizia "quantos" objetos havia neste conjunto, no total. Este parece ter sido o passo mais difícil. Se ao último dedo da segunda mão correspondia a última ovelha, havia "duas mãos" (ou "um homem") de ovelhas no total.

À medida que as civilizações evoluíam, o sistema se tornava mais exigente, com quantidades maiores a serem "contadas". E ficava uma pergunta: o que fazer quando a seqüência ordenada dos marcadores (dedos, partes do corpo, pedrinhas etc.) se esgota e ainda restam objetos a serem contados? Uma resposta seria: acrescentar mais marcadores (outras partes do corpo, mais pedrinhas); outra seria: estender a contagem por repetição; se "um homem" correspondia a 10 ovelhas (dedos das mãos), "dois homens" corresponderiam a 20 ovelhas, repetindo a contagem. Em símbolos, existiria um símbolo para cada coisa contada (por exemplo, um dedo) e um símbolo para cada grupo de coisas contadas (grupos de dez, ou doze, ou sessenta). O sistema de símbolos para cada grupo de coisas contadas aparece entre os babilônios, egípcios, gregos antigos e romanos. A repetição dos símbolos permitia a representação de (quase) qualquer número: surgem, assim, os sistemas de numeração.

**Enumeração**
[Do lat. *enumeratione*] S.f. 1.Indicação de coisas uma por uma. 2. Exposição ou relação metódica. 3. Conta, cômputo.
*Fonte: Dicionário Aurélio*

**Numeração**
[Do lat. *numeratione*] S.m. 1. Ato de numerar. 2. Série de números arábicos ou romanos que distinguem as páginas de livro, folheto, manuscrito etc. 3.Arit. Processo de enumerar um conjunto.
*Fonte: Dicionário Aurélio*

Essa necessidade de contagem deu origem à enumeração dos objetos; o conceito de *número* veio mais tarde. A linguagem serviu como um procedimento simplificador na evolução da *enumeração* para a numeração, dando origem aos sistemas de numeração.

Descrevemos, a seguir, alguns antigos sistemas de numeração:

1) **Egípcios** (há cerca de 5000 anos) - sistema aditivo, base dez. Tinham símbolos especiais para 1, 10, 100, 1000, 10 000, 100 000 e não havia símbolo para o zero; para expressar números muito grandes usavam também um sistema multiplicativo.

2) **Babilônios** (mesma época que os egípcios) - viviam na Mesopotâmia, entre os rios Tigre e Eufrates (atual Iraque); eram comerciantes e tinham necessidade de documentar suas atividades comerciais. Os números menores que 60 eram representados em base 10, por agrupamentos; os demais eram representados em base 60, pelo princípio posicional. A notação dava margem à mais de uma interpretação. Não havia um símbolo para o zero, mas eles deixavam um espaço para indicá-lo. Herdamos dos babilônios a representação das horas e das medidas de ângulos (base 60).

3) **Gregos** (cerca de 600 anos a.C.) - sistema aditivo, base 10. Usavam 27 símbolos: 24 eram as letras do alfabeto e 3 eram letras que, na época, já estavam em desuso. Além dos símbolos, usavam também acento nas letras; com isso, conseguiam representar números até 10 000 com apenas 4 letras e acentos.

4) **Romanos** (cerca de um século a.C.) - sistema aditivo, base 10. Também usavam letras do alfabeto para representar os números, por exemplo: I representava a quantidade 1, V representava a quantidade 5, L representava o 50 etc. Na época de Cristo, o sistema era somente aditivo (por exemplo, a representação do quatro: IIII); na idade média, incorporaram uma subtração para economizar símbolos (passaram a representar o 4 por IV, isto é: 5-1). Este sistema é usado até hoje.

5) **Chineses e japoneses** (cerca do século III a.C.) - sistema misto de aditivo e multiplicativo, base 10. Os números eram representados na escrita de cima para baixo, ou da esquerda para a direita. No início, os símbolos eram como os ideogramas; os cálculos eram feitos com barras estendidas sobre uma mesa, o que levou à utilização das barras como símbolos para representar os números, simplificando a notação. O novo sistema de barras era composto de 18 símbolos, usados numa espécie de sistema posicional. Um documento de 1247 mostra o lugar do zero ocupado por um círculo.

6) **Maias** (cerca do século IV d.C.) - sistema posicional, base 20; usavam traços e pontos para representar os números. Desenvolveram um calendário, conheciam astronomia, arquitetura e tinham grande atividade comercial.

## Atividade

1) Faça uma busca bibliográfica e consulte alguns livros que abordam os diferentes sistemas de numeração segundo os povos. Evidencie características de cada sistema como, por exemplo: os símbolos usados, a base, se o sistema é aditivo, multiplicativo ou posicional. Faça um resumo de, no máximo, duas páginas.

## O sistema indo-arábico

O nosso sistema de numeração é relativamente recente; antes da era cristã, cada civilização tinha seu próprio sistema, o que dificultava as atividades de comércio. Não podemos precisar exatamente a origem do nosso sistema; símbolos semelhantes aos nossos foram encontrados na Índia, em colunas de pedra de um templo construído por volta de 250 a.C. Nesta época, eram usados símbolos especiais para as potências de 10, mas, não há registro de um símbolo para o zero e a notação posicional não aparece. A maior parte dos historiadores situaram o final do desenvolvimento do sistema, com uso pleno e sistemático do zero e a notação posicional, entre os séculos IV e VII d.C.

Por volta do ano 800, o sistema foi levado a Bagdá e foi adotado pelos árabes. Por volta de 825, o persa al-Kowarizmi descreveu o sistema, atribuindo-o exclusivamente aos indianos. Ao se deslocarem através das costas do norte da África e depois até a Espanha, os árabes levaram estes trabalhos e também outras importantes obras gregas traduzidas para o árabe, difundindo a cultura grega na Europa. A obra de al-Kowarizmi perdeu-se, mas, existe uma tradução latina do século XII, – o *Liber Algorismi*, que contribuiu para a introdução do sistema e suas formas de calcular no mundo ocidental. Também as obras de Fibonacci – *Liber Abaci* e de Sacrobosco – *Algorismus Vulgaris*, do século XIII, descrevem o sistema e suas vantagens em relação ao sistema romano. Cópias manuscritas destes trabalhos podem ser

encontradas em muitas bibliotecas da Europa. A padronização dos símbolos que representam os números foi resultado da invenção da imprensa, em meados do século XV.

## Atividade

2) Faça um esquema, explicando o sistema posicional indo-arábico. Considere que este esquema você utilizará para explicar a estrutura do sistema posicional indo-arábico a uma pessoa leiga (Esquema deve ser simples e claro).

## 1.1.2 A evolução do estudo dos números

À medida que as antigas civilizações se desenvolveram, a necessidade de contar e registrar, despertou interesse pelos números e suas operações. Documentos antigos relatam listas de problemas e suas resoluções (o **papiro de Rhind**, por exemplo) em termos de cálculos: cada problema com sua resolução, sem generalizações.

Este papiro foi encontrado pelo egiptólogo inglês Rhind no final do século 19 e, hoje, está exposto no Museu Britânico, em Londres. FONTE: http://pt.wikipedia.org/wiki/Papiro_Rhind

Com a civilização grega surgiu o interesse pelas propriedades dos números, como registrado nos "*Elementos de Euclides*", de aproximadamente 300 a.C. Nesta obra, (uma compilação da matemática da época distribuída em treze Livros), com objetivo didático, já aparecem os conceitos de múltiplos, divisores e números primos, entre outros. Os Livros VII, VIII e IX tratam da aritmética teórica, porém, como era costume entre os gregos, o enfoque e a linguagem eram geométricos. Para eles, um número era um segmento, como podemos observar na definição 5 do Livro VII: "Um número é parte de outro, o menor do maior, quando ele mede o maior". Era assim que Euclides expressava que um número era divisor de outro. Conseqüentemente, definiam número primo como "Um número primo é aquele que é mensurável somente pela unidade" (definição 11 do Livro VII). *Mensurável* tinha o significado de *divisível*.

A organização dos "Elementos" é como a de qualquer livro atual que trata do assunto em nível superior: definições, teoremas, demonstrações. Muito do que é tratado nestes Livros se deve à escola Pitagórica; Pitágoras nasceu na ilha de Samos, por volta do ano 500 a.C., e, quando jovem, visitou demoradamente o Egito, a Índia e a Mesopotâmia. Em suas viagens absorveu muito de matemática e do

misticismo destes países em relação aos números; de volta à colônia grega de Crotona (sul da Itália), quando tinha cerca de 40 anos, fundou um misto de escola e comunidade religiosa onde cultivavam a Filosofia, a Ciência e a Matemática. A escola, apesar de dispersa por problemas políticos, continuou a existir através dos seguidores de Pitágoras (Filolaus e Arquitas de Tarento, entre outros) por, pelo menos, mais dois séculos após sua morte, em 497 a.C. Historiadores atribuem aos pitagóricos a criação de uma matemática "pura", no sentido de conter muito de filosofia e abstração, desvinculada dos problemas práticos: "aritmética" significava o estudo teórico dos números e, aos cálculos, os pitagóricos davam o nome de "logística". Atribui-se também aos pitagóricos certos conceitos como números figurados, números perfeitos e números amigos.

A partir de meados do século XIX, o interesse pelos números voltou-se para o estudo das "estruturas", como generalizações dos sistemas numéricos. Uma estrutura algébrica consiste num conjunto (cujos elementos não são necessariamente números) equipado com operações (operação no sentido de relacionar dois elementos com um terceiro) que satisfazem determinadas condições. O conjunto dos números inteiros munido das operações de adição e multiplicação é exemplo de uma estrutura que leva o nome de "anel"; tem a mesma estrutura de anel, o conjunto dos polinômios em uma variável com coeficientes inteiros, equipado com as operações de adição e multiplicação de polinômios.

Mais recentemente, a partir da segunda metade do século XX, o interesse pela teoria que trata de números deveu-se à sua aplicação em criptografia e códigos de segurança, mais especificamente, após o advento dos computadores. Antigos teoremas chineses foram resgatados e utilizados a fim de otimizar a linguagem das máquinas.

## Atividade

3) Pesquise e elabore um texto de no máximo 15 linhas sobre o que representou a Escola Pitagórica no contexto da evolução dos números.

4) Você sabe a definição de números amigos, figurados e perfeitos? Pesquise e faça o que se pede:

a) Defina números figurados e dê exemplos.

b) Defina números perfeitos e dê exemplos.

c) Dê a definição de números amigos e exemplifique.

Pesquise, você mesmo, uma bibliografia para consulta.

## 1.2 Sistemas posicionais: bases de sistemas de numeração

No presente estudo, buscamos oferecer para o aluno a compreensão da estrutura do sistema de numeração decimal, dos processos segundo os quais operamos e a compreensão da representação e tratamento em outros sistemas de numeração.

No ensino, os sistemas posicionais de bases diferentes da base 10 são estudados, pois este estudo permite compreender melhor as estruturas, os processos, segundo os quais operamos. A compreensão e uma conseqüente habilidade de tratamento dos processos são fundamentais para o professor de matemática.

Como vimos, a numeração escrita é muito antiga. A evolução da numeração encontra sua expressão final no sistema de numeração decimal.

O surgimento do sistema de numeração posicional, de base 10, foi provavelmente conseqüência do uso, praticamente universal, dos dez dedos das mãos.

Foram os Indianos que nos deram o inteligente método de expressar todos os números através de dez símbolos, cada símbolo recebendo tanto um valor posicional como um valor absoluto; uma idéia profunda e importante, ignorada durante muito tempo e que, agora, nos parece simples.

### 1.2.1 Bases de sistemas de numeração

Você está familiarizado a representar os números, não importa qual a quantidade, usando a posição dos algarismos: por exemplo 14, 357, 2389 etc. Desde o Ensino Fundamental você aprendeu a escrevê-

los, lê-los, a identificar as classes de cada um deles etc. Mas você já sabe que esta representação apóia-se em uma idéia matemática mais complexa? Qual é essa idéia?

Vejamos alguns exemplos:

**Exemplo 1.** O número 524 pode ser decomposto em

$$524 = 500 + 20 + 4.$$

Podemos representar esta decomposição por:

$$524 = 5.100 + 2.10 + 4.$$

Note que a maior potência de 10 menor do que 524 é a potência 2, ou seja, $10^2$ (centena): esta potência aparece 5 vezes no número 524. Temos que 524 consiste em 5 centenas, restando 24, o qual se constitui de 2 dezenas e 4 unidades. Assim temos: $524 = 5.10^2 + 2.10 + 4$.

**Exemplo 2.** O número 7031 pode ser decomposto em:

$$7.1000 + 0.100 + 3.10 + 1.$$

Neste caso, a maior potência de 10 menor do que 7031 é 3, ou seja, $10^3$ (milhar). Veja que a quantidade de centenas é zero, ou seja, 7031 consiste de 7 milhares, nenhuma centena, 3 dezenas e uma unidade. Assim temos: $7031 = 7.10^3 + 0.10^2 + 3.10 + 1$.

Para explorar a relação entre a maior potência de 10 de um número, propomos que você faça a decomposição conforme os exemplos anteriores, de diferentes números.

Observe também a relação entre a maior potência de 10 possível em cada número e a quantidade de algarismos do número. O que você descobriu?

Você sabe o que é um sistema de numeração decimal?

O que fizemos usando potências de 10 (no sistema de numeração decimal), podemos fazer usando potências de qualquer outro número?

No sistema de numeração decimal, trabalhamos com potências de 10, por isso, dizemos que nesse sistema a base é 10. Utilizamos 10 símbolos para representar os números: 0, 1, 2, 3, 4, 5, 6, 7, 8 *e* 9, chamados "algarismos" e mais recentemente "dígitos" (palavra derivada do latim que significa dedo). Se usarmos outro número como base, quantos símbolos usaríamos como algarismos? Você tem alguma idéia?

Observe: na base 10, temos 10 algarismos, de 0 a 9. Veja 9 = 10 -1 (número total de algarismos menos 1)

Agora vejamos como podemos representar genericamente um número qualquer no sistema decimal. Por exemplo: consideremos o número de 4 algarismos: *abcd*. Temos os algarismos *a*, *b*, *c* e *d*. Se este número está na base 10, teremos:

$$abcd = a.10^3 + b.10^2 + c.10 + d.$$

Compare com as representações do número 7031 feitas anteriormente.

O 10 indica a base. Veja que $abcd = a.10^3 + b.10^2 + c.10 + d$ . Esta maneira de expressar o número *abcd* chama-se *representação polinomial de abcd na base* 10.

Veja que num sistema posicional decimal, dependendo da posição, o algarismo representa unidades, dezenas, centenas, milhares etc.

Vejamos como fica a representação polinomial na base 10 de alguns números.

## Exercício resolvido

1) Dar a representação polinomial na base 10 dos seguintes números:

a) 5832

Notemos que $5832 = 5000 + 800 + 30 + 2$ e também temos que: $5000 = 5.10^3$ ; $800 = 8.10^2$ e $30 = 3.10$ . Assim,

$$5832 = 5.10^3 + 8.10^2 + 3.10 + 2 .$$

b) 142

Veja que $142 = 100 + 40 + 2 = 1.100 + 4.10 + 2 = 1.10^2 + 4.10 + 2$ .

Logo: $142 = 1.10^2 + 4.10 + 2$ .

c) 206

Temos que $206 = 200 + 0 + 6 = 2.100 + 0.10 + 6 = 2.10^2 + 0.10 + 6$ .

Portanto: $206 = 2.10^2 + 0.10 + 6$ .

## Exercício proposto: Agora é sua vez!

1) Dê a representação polinomial dos números:

a) 320

b) 20351

c) 7809354

E se estivermos trabalhando em outra base, como fica a representação polinomial?

## 1.2.2 Sistema de numeração posicional em bases diferentes da base decimal

Porque escolhemos a base 5? Foi a primeira idéia que ocorreu.

Começaremos estudando o sistema de numeração posicional de Base 5. Para trabalhar em base $5$, quantos algarismos devemos ter?

Em analogia com a representação dos números num sistema em base 10, devemos ter 5 algarismos. A quantidade de símbolos utilizada é igual ao número que representa a base.

Vamos, por escolha, usar os mesmos símbolos usados para a representação no sistema decimal.

Assim escreveremos todos os números na base 5 com os algarismos de 0 a 4, ou seja: 0, 1, 2, 3 e 4. O maior algarismo é 4, pois $5 - 1 = 4$.

Uma situação problema se coloca:

Como escrever na base 5 um número cuja representação está dada na base 10? E se quiséssemos representar esse número na base 3, na base 2 etc?

Na base 5 podemos usar os algarismos: 0, 1, 2, 3 e 4.

Vejamos por meio de exemplos:

Consideremos o número 87 na base 10. Queremos representá-lo na base 5. Isto é, qual a forma polinomial deste número na base 5?

De forma análoga ao que fizemos para determinar a representação polinomial dos números na base 10, determinamos a representação polinomial de um número dado em qualquer outra base. Para determinar a representação polinomial do 87 na base 5, seguimos os passos dados a seguir:

1) Determinar a maior potência de 5 em 87.
   Temos que em 87 "cabem" $3.5^2$ e ainda sobram 12.
2) Determinar a maior potência de 5 em 12.

Em 12 "cabem" 2.5 e sobra 2. Como 2 é um dígito, o processo termina.

Assim, $87 = 3.25 + 2.5 + 2$ ou $87 = 3.5^2 + 2.5 + 2.5^0$, que é a *representação polinomial do 87 na base 5*. Agora, identifiquemos nesta representação do 87, os coeficientes. Estes são os algarismos do número 87 na base 5. Temos então: 3, 2, 2. Assim o número 87 na base 5 será denotado por $(322)_5$.

Isto é, podemos escrever: $87 = (322)_5$. Lê-se: oitenta e sete é igual a três, dois, dois, na base 5.

Veja que os coeficientes das potências de 5 são os algarismos do número na base 5; o número após o parêntese indica a base. Quando a base não está explicitada significa que o número está na base 10.

Vejamos, agora, como achar a representação polinomial de um número na **Base 3:**

Na base 3, temos 3 símbolos: 0, 1, 2.

Como representar, por exemplo, 71 na base 3?

Temos que:

$$71 = 2.27 + 1.9 + 2.3 + 2 = 2.3^3 + 1.3^2 + 2.3 + 2.3^0,$$
$$\text{isto é, } 71 = (2122)_3.$$

Como representar, por exemplo, 87 na base 3?

$$87 = 1.81 + 0.27 + 0.9 + 2.3 + 0 = 1.3^4 + 0.3^3 + 0.3^2 + 2.3 + 0.3^0$$
$$\text{Assim, } 87 = (10020)_3.$$

Agora já sabemos que podemos representar o número 87 na base 5 e na base 3, ou seja,

$$87 = (87)_{10} = (322)_5 = (10020)_3.$$

Até aqui, trabalhamos com exemplos particulares. Genericamente, fixada uma base qualquer, podemos determinar a *representação polinomial nesta base* de qualquer número natural dado na base 10. Ou seja, escolhido um número natural $b > 1$ (como base), todo número natural $a$ pode ser representado, de forma única, do seguinte modo:

$$a = a_r b^r + a_{r-1} b^{r-1} + ... + a_2 b^2 + a_1 b + a_0$$

sendo $a_r, a_{r-1}, ..., a_2, a_1, a_0$ os algarismos de $a$ na base $b$. Estes assumem valores de $0$ $a$ $b-1$ (onde $b$ indica o número de símbolos); $b$ é a base do sistema de numeração e $r+1$ é o número de algarismos do número $a$.

A expressão $a = a_r b^r + a_{r-1} b^{r-1} + \ldots + a_2 b^2 + a_1 b + a_0$ com as condições descritas acima é a lei de formação do número $a = (a_r a_{r-1} \ldots a_2 a_1 a_0)_b$.

Na verdade, o resultado anterior é uma **proposição** que pode ser demonstrada. Não o faremos aqui por que ainda não temos elementos para tal. Aceitaremos o resultado motivado pelos exemplos que foram feitos e, também, pela boa quantidade de exemplos que serão resolvidos e propostos como exercício.

## Exercícios resolvidos

Como obter a representação na base *b* de um número *a* dado na sua representação decimal? Vamos estudar o procedimento a partir de exemplos.

2) Escrever 59 na base 2.

- Prestar atenção que sendo a base $2$, as potências deverão ser de base $2$.
- Determinar a maior potência de $2$, menor ou igual a $59$, ou seja, $2^5 = 32$. Efetuar a subtração $59 - 32 = 27$.
- Determinar a maior potência de $2$, menor ou igual a $27$ ou seja, $2^4 = 16$. Efetuar a subtração $27 - 16 = 11$.
- Determinar a maior potência de $2$, menor ou igual a $11 : 2^3 = 8$. Efetuar a subtração $11 - 8 = 3$.
- Determinar a maior potência de $2$ menor ou igual a $3 : 2^1$. Efetuar a subtração: $3 - 2 = 1$. Como $1$ é um algarismo encerra-se o processo.
- Contamos o número de vezes que aparece cada potência e escrevemos a lei de formação.

Logo temos: $59 = 1.2^5 + 1.2^4 + 1.2^3 + 0.2^2 + 1.2 + 1.2^0$.

Ou seja: $59 = (111011)_2$, onde cada algarismo é o coeficiente da potência de $2$ correspondente.

Confira: os algarismos de um número escrito na base $2$, são $0$ *e* $1$.

3) Escrever o número $59$ na base $3$.

- Determinar a maior potência de $3$, menor ou igual a $59$, ou seja: $3^3 = 27$. Efetuar a subtração $59 - 27 = 32$.
- Determinar a maior potência de $3$, menor ou igual a $32$ ou seja: $3^3 = 27$. Efetuar a subtração $32 - 27 = 5$.
- Determinar a maior potência de $3$, menor ou igual a $5$ ou seja: $3^1 = 3$. Efetuar a subtração $5 - 3 = 2$. Como $2$ é um algarismo, o processo termina aqui.

Vejamos: temos duas vezes a *3ª potência de* $3$, zero vezes a *2ª potência de* $3$, uma vez a *1ª potência de* $3$ e duas vezes a *potência zero de* $3$.

Assim: $59 = 2.3^3 + 0.3^2 + 1.3 + 2.3^0$, ou seja, $59 = (2012)_3$.

E para bases maiores do que 10 como fazer? Como representar na base 12, um número dado na base 10?

De acordo com o que vimos até agora sabemos que precisaremos de 12 símbolos. Consideremos então os símbolos: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, $a = 10$, $b = 11$ os algarismos para representar um número na base 12.

A escolha das letras $a$ e $b$ para representar os algarismos 10 e 11 é arbitrária.

- Determinar a representação de 160 na base 12.

  Sabemos que $144 = 12^2$, *e* $160 - 144 = 16$; $16 - 12 = 4$ logo temos:

  $$160 = 1.12^2 + 1.12 + 4.12^0 = (114)_{12}.$$

- Determinar a representação de $276$ na base $12$.

  Sabemos que $12^2 = 144$ *e* $276 - 144 = 132$.

  Mas em $132$ cabem $11$ pacotes de $12$, ou seja, $132 = 11.12$.

  Assim $276 = 1.12^2 + 11.12 + 0.12^0 = (1b0)_{12}$.

## Desafio

Qual é o número $(935)_{15}$ na base 10?

## Exercícios propostos

2) Escreva o número 25 na base 2.

3) Escreva o número 25 na base 3.

4) Escreva o número 59 na base 4.

5) Escreva o número 59 na base 5.

6) Escreva o número 25 na base 5.

7) Escreva o número 39 na base 7.

8) Escreva os números 132 e 87 na base 12.

9) Escreva o número $(322)_5$ na base 10.

## Atividade

5) Você é capaz, agora, de fazer alguma conjectura, ou de compreender possíveis dificuldades dos alunos de 5ª série, por exemplo, quanto à compreensão do sistema de numeração decimal? Discuta com seus colegas.

## Outro método para determinar a representação polinomial

Um outro procedimento para determinar a representação polinomial de um número numa base qualquer é utilizar divisões sucessivas.

Vejamos: Queremos representar o número 59 (base 10) na base 3. O que fazemos?

Iniciamos dividindo o 59 por 3. Em seguida vamos dividindo os quocientes por 3. Ou seja:

1) 59 |3
29 19
2

2) 19 |3
1 6

3) 6 |3
0 2

4) 2 |3
2 0

De onde temos:

- $59 = 19.3 + 2$; temos $19$ pacotes de $3$ e sobrou $2$.
- $19 = 6.3 + 1$; os $19$ pacotes de $3$ reagrupamos em $6$ pacotes de $3$ e sobra $1$;
- $6 = 2.3 + 0$; os $6$ pacotes de $3$ reagrupamos em $2$ novos pacotes $3$;
- $2 = 0.3 + 2$; os $2$ novos pacotes, para reagrupar em $3$, dá zero e continuo com os $2$ novos pacotes de $3$;

Isto é,

$$59 = 19.3 + 2 = (6.3 + 1).3 + 2 = [(2.3 + 0).3 + 1].3 + 2 =$$
$$= [(2.3 + 0).3 + 1].3 + (0.3 + 2) = 2.3^3 + 0.3^2 + 1.3 + 2.$$

Assim: $59 = (2012)_3$.

Os algarismos do número 59 na base 3 são os restos das divisões acima a contar da direita para a esquerda.

De modo geral, para representar na base *b* um número escrito na base 10 fazemos divisões sucessivas deste número por *b* até o quociente ser zero. Os algarismos da representação do número na nova base *b*, serão os restos das divisões a contar da direita para a esquerda (do último resto para o primeiro; por quê?).

**Observação:** como no sistema de numeração decimal você faz agrupamentos de 10 em 10, nos sistemas de numeração de outras bases a estrutura é a mesma, você sempre faz agrupamentos da quantidade correspondente ao valor da base. Assim como você opera com números na base 10, você poderá operar com números em quaisquer outras bases, pois, os procedimentos são completamente semelhantes àqueles utilizados na base 10.

## Exercícios propostos

Resolva os exercícios usando o procedimento das divisões sucessivas.

10) Escreva o número $59$ na base $5$.

11) Escreva o número $25$ na base $4$.

## 1.2.3 Operações nos sistemas de numeração de diferentes bases

Vamos estudar as operações de adição, subtração e multiplicação, usando representações de números em diferentes bases.

### Operações em base 10

**a) Adição: Determinar** $352 + 764$.

Segundo o algoritmo que estamos habituados a usar, fazemos:

$$\begin{array}{r} 352 \\ +\ 764 \\ \hline 1116 \end{array}$$

Somamos 4 + 2 = 6 unidades; 6 + 5 = 11, 11 dezenas, ou seja, 11 = 10 + 1 (10 dezenas mais 1 dezena), mas 10 dezenas é uma centena, por isso, somamos 1 às centenas. Assim temos: 3 + 7 + 1 = 11 centenas.

Vejamos como fica a adição usando a representação polinomial na base 10 dos números: 352 e 764.

**Resolução.** Sabemos que,

$$352 = (3.10^2 + 5.10 + 2.10^0) \text{ e,}$$

$$764 = (7.10^2 + 6.10 + 4.10^0). \text{ Assim,}$$

$$352 + 764 = (3.10^2 + 5.10 + 2.10^0) + (7.10^2 + 6.10 + 4.10^0).$$

Somando os coeficientes das potências iguais, temos:
$10.10^2 + 11.10 + 6.10^0$. Mas $11 = 10 + 1$ então, substituindo, temos:

$$\begin{aligned} 10.10^2 + 11.10 + 6 &= 10^3 + (10+1).10 + 6 = \\ &= 10^3 + 10.10 + 10 + 6 = \\ &= 1.10^3 + 1.10^2 + 1.10 + 6. \end{aligned}$$

Logo temos: $352 + 764 = 1116$.

Você percebeu, nesta operação, a história do "vai um"? Em que momento da operação você tratou desta questão?

Vejamos agora a multiplicação. Como exemplo, façamos a tarefa:

**b) Multiplicação: Determinar o produto:** $346 \times 13$

Pelo algoritmo que estamos habituados a usar, obtemos o seguinte resultado:

$$\begin{array}{r} 346 \\ \times\ 13 \\ \hline 1038 \\ 346 \\ \hline 4498 \end{array}$$

Explique passo a passo cada sub-resultado obtido ao efetuar esta operação. Justifique, por exemplo, os resultados obtidos ao multiplicar 3 por 6, 3 por 4 e 3 por 3; depois 1 por 6, por 4 e por 3 e como se chegou ao produto. Discuta com os colegas.

E como fica a multiplicação usando a representação polinomial dos números?

Sabemos que:

$$346 = (3.10^2 + 4.10 + 6) \quad \text{e} \quad 13 = (1.10 + 3).$$

Então:

$$346 \times 13 = (3.10^2 + 4.10 + 6) \times (1.10 + 3).$$

Pelas propriedades (associativa e comutativa da adição, e distributiva) de números naturais temos:

$$\begin{aligned} 346 \times 13 &= (3.10^2 + 4.10 + 6) \times (1.10 + 3) \\ &= 3.10^2.1.10 + 3.10^2.3 + 4.10.1.10 + 4.10.3 + 6.1.10 + 6.3 = \\ &= 3.10^3 + 9.10^2 + 4.10^2 + 12.10 + 6.10 + 10 + 8 = \\ &= 3.10^3 + 9.10^2 + 4.10^2 + (10+2).10 + 6.10 + 1.10 + 8 = \\ &= 3.10^3 + 9.10^2 + 4.10^2 + 1.10^2 + 2.10 + 6.10 + 1.10 + 8 = \\ &= 3.10^3 + 14.10^2 + 9.10 + 8 = \\ &= 3.10^3 + (10+4).10^2 + 9.10 + 8 = \\ &= 3.10^3 + 10^3 + 4.10^2 + 9.10 + 8 = \\ &= 4.10^3 + 4.10^2 + 9.10 + 8. \end{aligned}$$

Assim:

$$346 \times 13 = (3.10^2 + 4.10 + 6) \times (1.10 + 3) =$$
$$= 4.10^3 + 4.10^2 + 9.10 + 8 = 4498 .$$

E no caso da subtração? Vejamos um exemplo:

**c) Subtração: Determinar a diferença:** $148 - 76$

Sabemos que:

$$\begin{array}{r} 148 \\ -\ 76 \\ \hline 72 \end{array}$$

Explique como você justifica a um aluno a operação $4 - 7$. Para poder explicar a operação, precisamos compreender a estrutura do sistema de numeração posicional. O 4 na posição em que se encontra representa  dezenas. Mas o 7 também. Como tirar 7 dezenas de 4 dezenas? Precisamos recorrer às centenas. Tomamos a centena que está representada ao lado do 4 e como sabemos que ela representa 10 dezenas, vamos lê-la como 10 dezenas. Agora sim, podemos juntá-las com as 4 dezenas que já temos, ficando assim com 14 dezenas, das quais podemos tirar 7 dezenas.

Usando a representação na forma polinomial, como fica a subtração do exemplo anterior?

Vejamos:

$$148 = (1.10^2 + 4.10 + 8) \text{ e } 76 = (7.10 + 6) .$$

Logo:

$$148 - 76 = (1.10^2 + 4.10 + 8) - (7.10 + 6) =$$
$$= (10^2 + 4.10 - 7.10) + (8 - 6) =$$
$$= 1.10^2 + (4 - 7).10 + 2$$

mas $10^2 = 10.10$, então temos:

$$1.10^2 + (4 - 7).10 + 2 = 10.10 + (4 - 7).10 + 2$$
$$= (10 + 4 - 7).10 + 2 = 7.10 + 2$$

Ou seja: $148 - 76 = 72$.

## Operações em outras bases

Vejamos as operações, adição, subtração e multiplicação em outras bases, usando a representação polinomial dos números e o algoritmo.

**a) Adição: Resolver a seguinte adição:** $(134)_5 + (11)_5$

Usando a representação polinomial dos números, temos que:

$$(134)_5 = (1.5^2 + 3.5 + 4) \text{ e } (11)_5 = (1.5 + 1).$$

Logo temos: $(134)_5 + (11)_5 = (1.5^2 + 3.5 + 4) + (1.5 + 1)$ e aplicando propriedades de números naturais podemos escrever:

$$\begin{aligned}(1.5^2 + 3.5 + 4) + (1.5 + 1) &= 1.5^2 + (3+1).5 + (1+4)\\ &= 1.5^2 + 4.5 + 1.5 = 1.5^2 + (4+1).5 =\\ &= 1.5^2 + 5.5 = 1.5^2 + 5^2 =\\ &= 2.5^2 + 0.5^1 + 0.5^0.\end{aligned}$$

Portanto, $(134)_5 + (11)_5 = (200)_5$.

## Exercícios propostos

12) Efetue: $(243)_5 + (431)_5$.

13) Efetue: $(235)_6 + (452)_6$.

E a Multiplicação? Agora você já é capaz de deduzir sozinho o procedimento. Para ilustrar, faremos com você um exemplo:

**b) Multiplicação de números representados em uma base qualquer: Efetuar** $(531)_7$ x $(13)_7$

Usando a representação polinomial dos números na base 7, temos:

$$(531)_7 = (5.7^2 + 3.7 + 1) \ e \ (13)_7 = (1.7 + 3)$$

Assim:

$$\begin{aligned}(531)_7 \times (13)_7 = (5.7^2 + 3.7 + 1) \times (1.7 + 3) &= 5.7^3 + 15.7^2 + 3.7^2 + 9.7 + 1.7 + 3 =\\ &= 5.7^3 + (2.7 + 1).7^2 + 3.7^2 + (7+2)7 + 1.7 + 3 =\\ &= 5.7^3 + 2.7^3 + 1.7^2 + 3.7^2 + 7^2 + 2.7 + 1.7 + 3 =\\ &= 7.7^3 + 5.7^2 + 3.7 + 3 = 7^4 + 5.7^2 + 3.7 + 3 =\\ &= 1.7^4 + 0.7^3 + 5.7^2 + 3.7 + 3 = (10533)_7.\end{aligned}$$

Portanto: $(531)_7 \text{ x } (13)_7 = (10533)_7$

Vejamos o algoritmo:

a) $3\text{x}1 = 3$.

b) $3\text{x}3 = 9 = 7 + 2$, fica 2 vai 1.

c) $3\text{x}5+1 = 15+1 = 2.7+2 = (22)_7$.

d) $1\text{x}1 = 1$

e) $1\text{x}3 = 3$

f) $1\text{x}5 = 5$

Assim, temos:

$$\begin{array}{r} (531)_7 \\ \times \quad (13)_7 \\ \hline (2223)_7 \\ +\ (531\ )_7 \\ \hline (10533)_7 \end{array}$$

Note: $5+2 = 7 = 1.7+0.7^0 = (10)_7$.

E a Subtração? Ilustraremos com um exemplo.

**c) Subtração: Determine a diferença:** $(235)_8 - (173)_8$

Vejamos o procedimento de cálculo usando a representação polinomial dos números:

$$(235)_8 - (173)_8 = (2.8^2 + 3.8 + 5) - (1.8^2 + 7.8 + 3).$$

Efetuando operações nas respectivas potências temos:

1) $5-3=2$ o coeficiente de $8^0$.

2) Não podemos efetuar $3.8 - 7.8 = (3-7).8$ em, pois 3 é menor do que 7. Devemos então tomar um "pacote" de $8^2$ (*de* $2.8^2$) considerá-lo como 8 pacotes de 8 e somá-los com os 3 "pacotes" de 8. Assim, $3+8=11$ e agora $11-7=4$. Sobrou então $4.8$; logo o coeficiente de $8^1$ *é* 4.

3) Vamos, finalmente, determinar o coeficiente de $8^2 : 2.8^2$ subtraindo $1.8^2$ mais $1.8^2$ (pacote de $8^2$ que foi utilizado na etapa anterior) restam $0.8^2$, ou seja, o coeficiente de $8^2$ *é* $0$.

Então:

$$\begin{aligned}(235)_8 - (173)_8 &= (2.8^2 + 3.8 + 5) - (1.8^2 + 7.8 + 3) = \\ &= (2.8^2 + 3.8) - (1.8^2 + 7.8) + (5 - 3) = \\ &= (2.8^2) - (1.8^2) + (3 - 7).8 + 2 = \\ &= (1.8^2 + 1.8^2) - (1.8^2) + (3 - 7).8 + 2 = \\ &= (1.8^2) - (1.8^2) + (8 + 3 - 7).8 + 2 = \\ &= 0.8^2 + 4.8 + 2 = (042)_8 = (42)_8 .\end{aligned}$$

Logo: $(235)_8 - (173)_8 = (42)_8$.

Vejamos a resolução da maneira usual:

$$\begin{array}{r} (235)_8 \\ \underline{-\ (173)_8} \\ (042)_8 \ . \end{array}$$

Você pode explicar passo a passo a operação? Explique para um colega.

Você procedeu da mesma maneira que segue, abaixo?

a) $5 - 3 = 2$

b) 3 (pacotes de 8) menos (7 pacotes de 8). Se tenho 3 pacotes, o número não é suficiente para poder tirar 7 pacotes. O que fazer?

c) ao lado tenho 2 pacotes de 8 . 8. Tomo um destes, que tem 8 pacotes de 8, e somo com os 3 que já tenho. Isto me dá um total de 11 pacotes de 8.

d) $11 - 7 = 4$ e ficamos com 4 pacotes de 8.

e) Agora ainda temos $1.8^2 - 1.8^2 = 0.8^2$.

Portanto: $(235)_8 - (173)_8 = (042)_8$.

## Exercícios propostos

14) Resolva

a) $(235)_6 + (143)_6$

b) $(342)_6 \, x (14)_6$

c) $(431)_5 + (213)_5$

d) $(421)_5 \, x (13)_5$

e) $(1010)_2 - (101)_2$

f) $(6305)_7 \, x (35)_7$

15) Ao efetuar as operações acima, você viu que saber tabuada é importante! Construa então a tabuada da adição e da multiplicação em base 5 e base 7 e efetue operações utilizando estas tabuadas.

Tabela da tabuada da adição - base 5.

| + | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 1 | | | | | |
| 2 | | | | | |
| 3 | | | | | |
| 4 | | | | | |

Tabela da tabuada da multiplicação – base 7

| x | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| 1 | | | | | | | |
| 2 | | | | | | | |
| 3 | | | | | | | |
| 4 | | | | | | | |
| 5 | | | | | | | |
| 6 | | | | | | | |

16) Qual é o número $(70531)_8$ na base 10?

17) Escreva o número 183 nas bases 2, 7 e 9.

18) Considere um sistema posicional na base 12 com algarismos: $0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a = 10, b = 11$. Escreva o número 39 nesta base. Qual o número na base 10 representa o número: $(10ab)_{12}$.

19) Quais os números decimais que escritos na base 2 são representados por:

a) $(10101)_2$;

b) $(10001000)_2$;

c) $(1110011)_2$;

d) $(1001101)_2$.

20) Os sistemas de numeração podem ser caracterizados (até certo ponto) por possuir ou não as seguintes propriedades:

a) Aditivos;

b) Usam um símbolo para o zero;

c) É um sistema multiplicativo;

d) Usa subtração na representação dos números;

e) Sistema posicional (valor relativo).

Também os sistemas podem ser caracterizados por:

a) Número de símbolos;

b) Base;

c) Tipo de símbolos.

Dar as características dos sistemas: dos Maias, Japoneses, Chineses, Romanos, Babilônicos, Egípcios e Gregos.

# Resumo

Neste capítulo, estudamos um pouco da História dos Números e dos Sistemas de Numeração de diferentes povos. Estudamos os números decimais em diferentes bases, e mostramos como determinar a representação polinomial de um número numa base dada. Também exploramos os algoritmos das operações de adição, multiplicação e subtração em bases diferentes da decimal.

Situamos neste estudo a problemática propulsora que levou à formulação dos sistemas de numeração bem como sua evolução desde a concepção até o estabelecimento do sistema de numeração decimal como universal.

# Capítulo 2

## Conjuntos Numéricos – Naturais e Inteiros

# Capítulo 2

## Conjuntos Numéricos – Naturais e Inteiros

*Apresentar os conjuntos dos números naturais e inteiros. Dar uma visão de suas estruturas. Abordar as operações definidas e as propriedades aritméticas, sendo estas, na medida do possível, rigorosamente justificadas.*

Neste capítulo, além de compreender definições e propriedades, você vai aprender a demonstrar grande parte das propriedades, justificando cada passagem.

Você verá que, neste capítulo, são poucos os exercícios propostos. Por que será?

Como já vimos no capítulo anterior, a humanidade passou por um percurso longo até chegar à formulação do sistema de numeração decimal. No continuar da caminhada até a formulação do conjunto dos números naturais, como conhecemos hoje, outro longo período de explorações, estudos, ensaios, tem lugar. A formulação axiomática do conjunto dos números naturais, isto é, uma formulação estrutural, formal, via os conceitos primitivos, axiomas, operações, propriedades, foi dada por Giuseppe Peano em 1889.

A estrutura elaborada por Peano teve como princípio o fato de que os números naturais podem ser ordenados de forma que cada elemento tem um sucessor.

No texto, a seguir, vamos levar algumas horas para conhecer um pouco sobre números naturais e sobre o conjunto dos inteiros, conteúdos que nossos antepassados levaram séculos para formalizar.

# 2.1 Conjunto dos números naturais

Como já sabemos, em 1889, Guiseppe Peano formaliza o conjunto dos números naturais. Eles surgiram com a necessidade de contagem. Tem por conceitos primitivos: o conceito do zero, de número natural e o conceito da relação *"é sucessor de"*.

São cinco os axiomas que formam a base da estrutura dos números naturais:

**Axioma 1.** Zero é um número natural.

Este axioma garante que o conjunto dos naturais é diferente do vazio, ou seja, o zero pertence ao conjunto dos naturais.

**Axioma 2.** Se $a$ é um número natural, então $a$ tem um único **sucessor** que também é um número natural (Representamos o sucessor de $a$ por $a^+$).

Um número natural $b$ é sucessor de $a$, se $b = a + 1$. Por exemplo: o número 6 é o sucessor de 5, pois $6 = 5 + 1$.

**Axioma 3.** Zero não é sucessor de nenhum número natural.

**Axioma 4.** Se dois números naturais têm sucessores iguais, então eles próprios são iguais. Em uma representação simbólica escrevemos: $a^+ = b^+ \Rightarrow a = b$.

Como conseqüência, temos: se $a$ é diferente de $b$ então o sucessor de $a$ é diferente do sucessor de $b$. Em uma linguagem simbólica: $a \neq b \Rightarrow a^+ \neq b^+$.

**Axioma 5.** Se uma coleção S de números naturais contém o zero e também o sucessor de todo elemento de S, então S é o conjunto de todos os naturais.

Este último axioma é chamado *axioma da indução completa*. Ele nos diz que se temos um conjunto S de números que contém o zero e, para cada um dos elementos deste conjunto, seu sucessor também está no conjunto S, então este conjunto é o próprio conjunto dos números naturais. Assim, como zero está em S, seu sucessor 1 também está em S; repetindo o argumento segue que 2 (o sucessor de 1) está em S; repetindo o argumento sucessivamente concluímos que:

$0,\ 1,\ 2,\ 3,\ 4,\ \ldots$, ou seja, todos os naturais estão em *S*. Deste modo, segue que S é o conjunto de todos os naturais.

Para representar o conjunto dos números naturais utiliza-se o símbolo $\mathbb{N}$ e para representar o zero, o símbolo 0. Como já vimos, para representar o sucessor de um número $a$, usamos o símbolo $a^+$.

Pelo raciocínio desenvolvido acima, o axioma 5 nos permite obter um conjunto de números: $\{0, 1, 2, 3, 4, 5, 6, 7, ...\}$ o qual é chamado conjunto dos números naturais e denotado por $\mathbb{N}$. Assim, temos que:

$$\mathbb{N} = \{0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ \ldots\}.$$

Em síntese, a partir dos axiomas, temos as seguintes afirmações:

1) O zero pertence a $\mathbb{N}$. Usando linguagem simbólica: $0 \in \mathbb{N}$.
2) Se $a$ pertence a $\mathbb{N}$ então o sucessor de $a$, $a^+$, pertence a $\mathbb{N}$. Em linguagem simbólica: $a \in \mathbb{N} \Rightarrow a^+ \in \mathbb{N}$.
3) Para todo número natural *a*, o sucessor de $a$ é diferente de zero. Em linguagem simbólica: $(\forall a \in \mathbb{N}) a^+ \neq 0$.
4) Sejam $a$ e $b$ dois números naturais; se o sucessor de $a$ é igual o sucessor de $b$ então $a$ é igual a $b$. Na notação simbólica: $a^+ = b^+ \Rightarrow a = b$.
5) Se $a$ é um número natural e $a \neq 0$, então existe um número natural $b$ tal que $a = b^+$. Isto significa que todo número natural não nulo é sucessor de algum número natural.
6) Se para um subconjunto S dos números naturais (denotaremos por: $S \subset \mathbb{N}$) estão satisfeitas as condições:
   i) O zero pertence a S;
   ii) Para todo $a$ pertencente a S, o sucessor de *a* pertence a S; então S é igual a $\mathbb{N}$.

Em linguagem simbólica:

$$(0 \in S) \wedge (\forall a \in S \Rightarrow a^+ \in S) \Rightarrow S = \mathbb{N}.$$

Com estes cinco axiomas, podemos estabelecer todos os fatos importantes de $\mathbb{N}$: operações, propriedades, enfim, toda "estrutura" do conjunto dos naturais, inclusive a relação de ordem "menor ou igual". Uma propriedade que decorre imediatamente dos axiomas é a seguinte: se um número natural $a$ é diferente de 0, então este número é sucessor de algum número natural. Por exemplo: como 56 é diferente de zero, ele é o sucessor de algum número natural, que sabemos ser o 55. Este fato será utilizado na definição das operações adição e multiplicação.

Agora já conhecemos o conjunto dos números naturais:

$\mathbb{N} = \{0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ \ldots\}$. Quando considerarmos o conjunto dos números naturais sem o elemento zero, isto é, se estivermos tratando de $\mathbb{N} - \{0\}$, indicaremos este conjunto por $\mathbb{N}^*$. Assim: $\mathbb{N}^* = \{1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ \ldots\}$.

## 2.1.1 Que operações estão definidas no conjunto dos números naturais?

No conjunto dos números naturais duas operações são definidas: a adição e a multiplicação.

Estas operações são regras, leis, que a cada par de elementos $(x, y)$, associa um elemento do conjunto $\mathbb{N}$.

**Como é definida a adição em $\mathbb{N}$?**

A definição formal da adição em $\mathbb{N}$ é baseada no conceito de sucessor.

A **adição** é uma função que leva cada par de números naturais $(x, y)$ à soma $x + y$, ou seja, é a função representada por +, que associa ao elemento $(x, y)$ de $\mathbb{N}$x$\mathbb{N}$ o elemento $x + y$ *de* $\mathbb{N}$.

$x$ e $y$ são chamados parcelas

$$\text{Simbolicamente: } \begin{array}{l} +: \mathbb{N} \times \mathbb{N} \to \mathbb{N} \\ (x, y) \mapsto x + y \end{array}$$

$$\text{onde } x + y = \begin{cases} x, \ se\ y = 0 \\ x + b^+ = (x + b)^+, \ se, \ y \neq 0 \ e \ y = b^+ . \end{cases}$$

**Exemplo:** Consideremos o par $(3,2)$ pertencente a $\mathbb{N}x\mathbb{N}$; segundo a definição dada, temos:

$$3+2=(3+1^+)=(3+1)^+=(3+0^+)^+=[(3+0)^+]^+=(3^+)^+=4^+=5.$$

Portanto ao par de números naturais $(3,2)$ associamos o número $5$. De forma simplificada, representamos por: $3+2=5$.

Note que na definição, se $y$ é diferente de zero, estamos usando o fato que ele é o sucessor de um número $b$ (propriedade que decorre dos axiomas).

**Como é definida a multiplicação em $\mathbb{N}$?**

A multiplicação é definida como uma função que associa cada par $(x,y)$ de números naturais ao número natural $x.y$. Ela é uma conseqüência da adição de parcelas iguais e é definida por:

$$\cdot : \mathbb{N}\times\mathbb{N}\to\mathbb{N}$$
$$(x,y)\mapsto x.y$$

$$x.y=\begin{cases}0, \ se\ x=0\ e\\ b^+y=by+y, \ se, \ x\neq 0\ e\ x=b^+\end{cases}$$

**Exemplo:** $2.3=1^+.3=1.3+3=0^+.3+3=0.3+3+3=0+3+3=6$.

**Propriedades da adição e da multiplicação em $\mathbb{N}$**

As propriedades aqui apresentadas não serão demonstradas, uma vez que para demonstrá-las precisaríamos da construção formal do conjunto $\mathbb{N}$. Vamos considerá-las como axiomas.

**Propriedades da adição em $\mathbb{N}$**

Seja então a adição uma operação que a cada par $(x,y)$ associa o número $x+y$, conforme a definição de "+" dada anteriormente e, $x, y$ e $z$ números naturais. As seguintes propriedades são válidas:

A1) **Propriedade associativa da adição**: $x+(y+z)=(x+y)+z$.

Você já tentou adicionar mais de dois números ao mesmo tempo?

Nós adicionamos os números aos pares. A propriedade associativa além de organizar a operação aos pares, garante que não importa a seqüência que tomamos as parcelas para adicionar.

A2) **Propriedade comutativa da adição**: $x + y = y + x$.

Isto é, podemos trocar as posições dos números que queremos adicionar e o resultado, no caso a soma, não se altera.

A3) **Propriedade do elemento neutro da adição**: Existe um elemento de $\mathbb{N}$ que satisfaz $x + 0 = 0 + x = x$.

Isto é: adicionando o zero a um número natural $x$ qualquer, obtemos como soma o próprio valor de $x$. Por isso diz-se que o zero é elemento neutro da adição em $\mathbb{N}$.

Por exemplo: $7 + 0 = 7$ (por definição) e $0 + 7 = 7 + 0$ (pela propriedade comutativa). Logo: $0 + 7 = 7 + 0 = 7$.

A4) **Lei do cancelamento da adição**: se $x, y$ e $a$ são naturais, então $x + a = y + a$ se, e somente se, $x = y$.

A5) **Lei do anulamento**: $x + y = 0$ se e somente se $x = y = 0$.

## Exercício resolvido

1) Efetue mentalmente as operações dadas abaixo. Em seguida, escreva a expressão numérica usada na resolução mental que você realizou.

a) $765 + 372$

$$[(700 + 300) + (60 + 70) + (5 + 2)] = 1000 + 130 + 7 = 1130 + 7 = 1137$$

Realizamos uma decomposição dos números:

$$765 + 372 = 700 + 60 + 5 + 300 + 70 + 2$$

$$765 + 372 = 700 + 60 + 5 + 300 + 70 + 2 =$$
(propriedade comutativa da adição)

$$= 700 + 300 + 60 + 70 + 5 + 2 =$$
(propriedade associativa da adição)

$$= [(700 + 300) + (60 + 70) + (5 + 2)]$$

$$= [1000 + 130] + 7 = 1130 + 7 = 1137 .$$

b) $89 + 54$

Podemos usar duas estratégias:

i) $89 + 50 + 4 = (89 + 1) + 50 + 3 =$

$$= [(89 + 1) + 10] + 43 = 100 + 43 = 143$$

ii) $(80 + 50) + (9 + 4) = 130 + 13 = 143$

**Propriedades aplicadas: comutativa e associativa da adição.**

Escolhemos organizações da expressão numérica que consideramos mais convenientes para o processo cognitivo de efetuar as operações.

## Exercício proposto

1) Efetue mentalmente, depois escreva a expressão numérica utilizada na operação e indique as propriedades manipuladas no processo.

a) $5709 + 697$

b) $350 + 528$

c) $9 + 88$

Quando efetuamos uma operação mental, usamos com muita naturalidade as propriedades comutativa e associativa da adição, entre outras. As propriedades são ferramentas que usamos no nosso dia-a-dia e não, somente, componentes da estrutura teórica dos conjuntos numéricos.

**Propriedades da multiplicação em $\mathbb{N}$**

Sejam $x, y$ e $z$ números naturais, e a multiplicação em $\mathbb{N}$, conforme definida anteriormente.

M1) **Propriedade comutativa da multiplicação:** $x.y = y.x$ .

M2) **Propriedade do elemento neutro da multiplicação**: Existe $1 \in \mathbb{N}$ tal que $x.1 = 1.x = x$.

Por exemplo: $8.1 = 1.8 = 8$. Qualquer número natural $x$ multiplicado por 1 tem como produto o próprio número $x$.

M3) **Propriedade associativa da multiplicação**: $(x.y).z = x.(y.z)$.

Uma vez que temos definidas as operações adição e multiplicação, podemos apresentar a propriedade distributiva. Esta envolve duas operações.

M4) **Propriedade distributiva** (também conhecida por "colocar em evidência"): sejam $x, y$ e $z$ números naturais. Então:

a) $(x + y).z = xz + yz$ (chamada distributiva à direita).

b) $x.(y + z) = xy + xz$ (chamada distributiva à esquerda).

Esta distinção entre distributiva à direita e distributiva à esquerda não é feita em geral. Normalmente tratamos de "propriedade distributiva."

**E a subtração e a divisão em $\mathbb{N}$?**

A subtração e a divisão não estão definidas como operação em $\mathbb{N}$ para quaisquer dois números do conjunto $\mathbb{N}$.

Vamos ver mais detalhadamente a seguir.

Para entendermos a subtração precisamos, antes, do conceito da Relação de ordem "$\leq$" definida em $\mathbb{N}$.

## 2.1.2 Definição da Relação de ordem

Sejam $a$ e $b$ pertencentes a $\mathbb{N}$; diz-se que $a \leq b$ quando existe um número natural $x$ tal que $b = a + x$.

**Observação:** você pode pensar neste $x$ como a quantidade que falta ao número $a$ para atingir $b$.

**Definição de diferença**: Sejam $a$ e $b$ números naturais e $a \leq b$; dizemos que a diferença $b-a$ é o número $x$ tal que $b = a + x$.

O elemento *b* é chamado de *subtraendo* e o elemento *a* é chamado de *minuendo*.

Notemos que a diferença $b-a$ somente está definida em $\mathbb{N}$ se $a \leq b$.

Isto quer dizer que a relação que associa ao par $(a,b)$ o elemento $(b-a)$ não é uma função. Portanto a subtração não é uma operação em $\mathbb{N}$. Por exemplo: não há como calcular $2-3$ no universo dos números naturais.

Também em $\mathbb{N}$, definimos a relação "menor": se $a$ e $b$ são números naturais, $a$ é menor do que $b$, se, e somente se, existe $x$ diferente de zero, tal que $b = a + x$.

Simbolicamente: $a < b \Leftrightarrow \exists x \neq 0$ tal que $b = a + x$.

**E a divisão em $\mathbb{N}$?**

Em geral, tratamos a divisão em $\mathbb{N}$ com tal naturalidade que nem nos damos conta que ela não é definida em $\mathbb{N}$.

**Nota:** Os casos de divisibilidade e o algoritmo da divisão serão vistos no capítulo 3.

Vejamos agora as propriedades da relação "$\leq$".

**Propriedades da relação "$\leq$":**

A relação "**menor ou igual**" satisfaz as seguintes propriedades:

1. **Reflexiva:** para todo *a* natural, $a \leq a$.

   **Demonstração.**

   Sabemos que: se $a \leq b$, existe $x$ pertencente a $\mathbb{N}$, tal que $b = a + x$. Tomemos $x = 0$, e teremos $a = a + 0$, isto é $a \leq a$.

   ■

2. **Anti-simétrica:** se $a,b$ são naturais tais que $a \leq b$ e $b \leq a$, então $a = b$.

**Demonstração.**

Hipótese: $a \leq b$ e $b \leq a$.

Tese: $a = b$.

Por hipótese, $a \leq b$ e $b \leq a$. Logo existem $x$ e $y$ naturais tais que $a + x = b$ e $b + y = a$.

Mas,

$$a = a + 0 = b + y = (a + x) + y = a + (x + y) \Rightarrow a + 0 = a + (x + y).$$

Assim, pela lei do cancelamento da adição segue que $x + y = 0$, portanto, $x = y = 0$ (pela lei do anulamento); então segue que $a = b$.

■

3. **Transitiva:** sejam $a$, $b$ e $c$ números naturais: se $a \leq b$ e $b \leq c$ então $a \leq c$.

**Demonstração.**

Hipótese: $a \leq b$ e $b \leq c$.

Tese: $a \leq c$.

A partir da hipótese, temos que existem $x$ e $y$ naturais tais que:
$b = a + x$ e $c = b + y$.

Logo, $c = b + y = (a + x) + y = a + (x + y)$. Como $x$ e $y$ são naturais $x + y = z$ é natural e $c = a + z$. Portanto (pela definição de $\leq$), $a \leq c$.

■

**Definição.** Uma relação definida num conjunto S satisfazendo as propriedades: Reflexiva, Anti-simétrica e Transitiva, é chamada uma *"Relação de ordem em S"*.

Acabamos de mostrar que as propriedades Reflexiva, Anti-simétrica e Transitiva são verdadeiras para a relação "**menor ou igual**", definida em $\mathbb{N}$. Logo a relação "menor ou igual" em $\mathbb{N}$ é uma relação de ordem em $\mathbb{N}$. Além disso, é uma relação de ordem *total*, o que significa que dados $a$ e $b$ naturais, $a \leq b$ ou $b \leq a$.

## 2.2 Conjunto dos números inteiros – uma ampliação dos números naturais

Consideramos a adição $a+x=b$, $a$, $x$ e $b$ naturais. Em particular, consideremos: $a=6$ e $b=1$. Assim $6+x=1$ ou então $x=1-6$. Como $1<6$, a diferença $1-6$ não está definida no conjunto dos naturais.

Esta dificuldade encontrada, isto é, a necessidade de se efetuar a subtração para quaisquer dois números naturais, foi um dos fatos que impulsionou o estudo que levou à formalização dos números inteiros.

O que se fez?

Ao conjunto dos números naturais acrescentaram-se todas as "diferenças" $b-a$ com $b$ menor do que $a$, formando um novo conjunto. Os elementos deste novo conjunto serão diferenças $b-a$, com $a$ e $b$ naturais. Observemos as diferenças $b-a$ onde $a$, $b \in \mathbb{N}$:

| | | | | |
|---|---|---|---|---|
| 0-0 | 0-1 | 0-2 | ... | 0-a |
| 1-0 | 1-1 | 1-2 | ... | 1-a |
| 2-0 | 2-1 | 2-2 | ... | 2-a |
| 3-0 | 3-1 | 3-2 | ... | 3-a |
| ⋮ | ⋮ | ⋮ | ... | ⋮ |
| b-0 | b-1 | b-2 | ... | b-a |
| ⋮ | ⋮ | ⋮ | ... | ⋮ |

Observe que algumas diferenças se repetem: 1-0; 2-1;... por exemplo. A primeira coluna representa o próprio conjunto $\mathbb{N}$ e a primeira linha gera os opostos dos elementos de $\mathbb{N}$, os números negativos. As outras diferenças todas são repetições.

O conjunto das diferenças: $0-1;\ 1-2;\ 2-3;\ 3-4;\ldots$ é representado pelo inteiro $-1$ (notação inspirada na diferença $0-1$).

Analogamente, o conjunto das diferenças: $0-2;\ 1-3;\ 2-4;\ldots$ é representado por $-2$. Assim sucessivamente, para cada seqüência de diferenças, associamos um elemento do conjunto dos inteiros.

Denotamos o novo conjunto por $\mathbb{Z}$ e o representamos por:

$$\mathbb{Z} = \{\ldots, -5, -4, -3, -2, -1,\ 0,\ 1,\ 2,\ 3,\ 4,\ 5, \ldots\}.$$

Geometricamente, representamos o conjunto dos números inteiros por pontos em uma reta; por exemplo:


Como $\mathbb{Z}$ é uma extensão de $\mathbb{N}$, o conjunto $\mathbb{N}$ está contido em $\mathbb{Z}$.

A representação de $\mathbb{Z}$ como pontos de uma reta facilita a compreensão das operações adição e subtração em $\mathbb{Z}$, que veremos a seguir.

Vejamos alguns subconjuntos de $\mathbb{Z}$, com sua respectiva representação, os quais são destacados em diferentes situações de aprendizagem:

- Inteiros não negativos: $\mathbb{Z}_+ = \{0,\ 1,\ 2,\ 3,\ 4,\ 5, \ldots\}$.
- Inteiros positivos: $\mathbb{Z}_+^* = \mathbb{Z}_+ - \{0\} = \{1,\ 2,\ 3,\ 4,\ 5, \ldots\}$.
- Inteiros não positivos: $\mathbb{Z}_- = \{0, -1, -2, -3, -4, -5, \ldots\}$.
- Inteiros negativos: $\mathbb{Z}_-^* = \mathbb{Z}_- - \{0\} = \{-1, -2, -3, -4, -5, \ldots\}$.

## 2.2.1 Operações em $\mathbb{Z}$

Em $\mathbb{Z}$ estão definidas as operações de adição, a multiplicação e a subtração.

**Adição:**

$$+ : \mathbb{Z} \text{x} \mathbb{Z} \to \mathbb{Z}$$
$$(a, b) \mapsto a + b$$

$a+b$ é a soma ou total e $a$ e $b$ são as parcelas.

**Propriedades da adição em $\mathbb{Z}$**

Apresentaremos, a seguir, as propriedades da adição em $\mathbb{Z}$; como fizemos para os naturais, elas serão abordadas como axiomas (isto é, serão aceitas sem demonstração).

A1) **Propriedade associativa da adição**:

Para todos $a, b$ e $c$ inteiros, temos $a+(b+c)=(a+b)+c$. Você alguma vez já refletiu sobre isto? Você somente pode efetuar uma operação de adição com mais de duas parcelas porque existe a propriedade associativa. Ou seja, cada vez que você efetua uma operação de adição com mais de duas parcelas você está usando a propriedade associativa da adição.

Assim, esta propriedade é importante pois permite somar mais de dois números.

Com esta propriedade, também descobrimos que basta sabermos somar a um número $a$ inteiro qualquer o número 1 ou $-1$, para sermos capazes de resolver qualquer adição. Vejamos por exemplo:

a) $3+2=3+(1+1)=(3+1)+1=4+1=5$.

b) $3+(-2)=3+[(-1)+(-1)]=[3+(-1)]+(-1)=2+(-1)=1$.

A2) **Propriedade comutativa da adição:**

Para todos $a, b$ pertencentes a $\mathbb{Z}$ temos $a+b=b+a$.

Lembre que "juntar" nem sempre é uma operação comutativa! Você poderia dar um exemplo onde a comutatividade não funciona? Pense, por exemplo, na Química.

A3) **Propriedade da Existência do elemento neutro:**

Existe um único elemento em $\mathbb{Z}$, denominado zero e denotado por 0, tal que $a+0=a$ para todo $a$ pertencente a $\mathbb{Z}$.

A4) **Propriedade da Existência do elemento oposto:**

Para cada inteiro $a$, existe um único inteiro $b$ tal que $a+b=0$.

Este número $b$ é chamado *"oposto de $a$"* e denotado por $-a$.

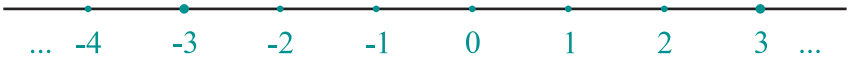
Observe que o oposto de $a$ é o único inteiro que satisfaz a equação $a+x=0$.

Não confunda a notação $-a$ com o "sinal de menos". Poderíamos denotar o oposto por qualquer outro símbolo, por exemplo, $a^*$. A notação $-a$ é usada por ser mais conveniente.

Geometricamente, o oposto de um número inteiro $a$ é aquele que, na reta, ocupa posição simétrica em relação ao zero.


$a$ e seu oposto estão à mesma distância do zero, em sentidos opostos.

**Exemplo:** O oposto de $-3$ é $3$ e vice versa.




**Multiplicação em $\mathbb{Z}$**

A multiplicação em $\mathbb{Z}$ deriva da adição em $\mathbb{Z}$ (soma de parcelas iguais).

Vejamos por exemplo: $4+4+4=3x4$

$$2+2+2+2+2=5x2.$$

Definimos a multiplicação em $\mathbb{Z}$ pela função:

$$\cdot : \mathbb{Z}x\mathbb{Z} \to \mathbb{Z}$$
$$(a,b) \mapsto a.b$$

onde $a.b$ é o produto e $a$ e $b$ são os fatores.

**Propriedades da multiplicação**

M1) **Propriedade associativa da multiplicação:**

Para todos $a,b$ e $c$ inteiros temos $(a.b).c = a.(b.c)$.

Com esta propriedade, podemos multiplicar mais de dois números. Ela é útil também para a notação de potências, que é um caso de multiplicação de fatores iguais.

Por exemplo: $3.3.3.3.3 = 3^5$.

M2) **Propriedade comutativa da multiplicação:**

Para todos $a, b$ inteiros, $a.b = b.a$.

M3) **Propriedade do elemento neutro da multiplicação:**

Existe um único elemento em $\mathbb{Z}$, denotado por $1$, tal que $1.a = a$ para todo $a$ inteiro.

D) **Propriedade distributiva:**

Para todos $a, b$ e $c$ inteiros, temos:

1) $a.(b+c) = a.b + a.c$ ; (distributiva a direita).

2) $(b+c).a = b.a + c.a$ ; (distributiva a esquerda).

Como já foi visto em $\mathbb{N}$, esta propriedade é também conhecida como "colocar em evidência". Por exemplo:

$$2.10^2 + 5.10 = 10.(2.10 + 5).$$

CM) **Propriedade do cancelamento da multiplicação:**

Para todos $a, b$ e $c$ inteiros, com $c \neq 0$, temos que,

$$\text{se } a.c = b.c \text{ então } a = b.$$

Vamos estudar, agora, outras propriedades importantes em $\mathbb{Z}$. Tenha sempre em mente que todas estas propriedades das operações nos conjuntos dos números naturais e inteiros serão úteis nos próximos capítulos: elas constituem a "caixa de ferramentas" necessária para a construção do conceito de divisibilidade do capítulo 3 e todas as suas conseqüências.

Todas as outras propriedades das operações em $\mathbb{Z}$ derivam destas, isto é, todas as outras propriedades podem ser provadas a partir das propriedades A1, A2, A3, A4, M1, M2, M3, D e CM, como será demonstrado mais adiante.

P1) **Lei do cancelamento da adição: Para todos inteiros** $a, b$ e $c$, se $a + c = b + c$ então $a = b$.

**Demonstração.**

Hipótese: $a, b$ e $c$ são números inteiros e $a + c = b + c$.

Tese: $a = b$.

Sejam $a, b$ e $c$ inteiros e a $a + c = b + c$. Como $c$ pertence a $\mathbb{Z}$, existe o oposto de $c$, ou seja, existe o número inteiro $-c$. Somando o oposto de c aos dois membros da igualdade $a + c = b + c$, obtemos:

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

Usando a propriedade associativa A1, obtemos

$$a + [c + (-c)] = b + [c + (-c)];$$

como $c + (-c) = 0$ (pela condição do oposto), temos $a + 0 = b + 0$ e pela propriedade do elemento neutro (A3), segue que $a = b$.

■

P2) **Para todo inteiro** $a$, **tem-se** $a.0 = 0.a = 0$.

**Demonstração.**

Hipótese: $a$ é um número inteiro qualquer.

Tese: $a.0 = 0.a = 0$.

De fato: seja $a$ um número inteiro. Pela propriedade do elemento neutro da adição temos que:

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

Mas pela propriedade distributiva, $a.(0 + 0) = a.0 + a.0$. Logo,

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

Agora, aplicando a propriedade do cancelamento da adição temos: $0 = a.0$. De modo análogo prova-se que $0.a = 0$.

■

P3) **Para todo inteiro** $a$**, tem-se** $(-1).a = -a$**.**

**Demonstração.**

Hipótese: $a$ é um número inteiro qualquer.

Tese: $(-1).a = -a$.

Seja $a$ um número inteiro. Sabemos que o oposto de $a$ é o único inteiro que satisfaz a equação $a + x = 0$. Como $0.a = 0$ (por $P_2$), segue que

$$0 = 0.a = [1 + (-1)].a = 1.a + (-1).a = a + (-1).a,$$

Conseqüentemente, o oposto de $a$ é $(-1).a$, ou seja $-a = (-1).a$.

■

P4) **Para todos $a, b$ inteiros, se $a.b = 0$ então $a = 0$ ou $b = 0$.**

**Demonstração.**

Para provar um "*ou*" numa proposição do tipo *Se p então* $(q$ *ou* $r)$, supomos que $q$ não ocorra (negamos $q$) e concluímos que $r$ ocorre.

Hipótese: $a, b$ inteiros e $a.b = 0$.

Tese: $a = 0$ ou $b = 0$.

Sejam $a$ e $b$ inteiros e $a.b = 0$ (hipótese). Então, por P2, temos $a.b = a.0$ e $a.b = b.0$.

Se $a \neq 0, e\ a.b = a.0$, pela lei do cancelamento da multiplicação, temos $b = 0$.

Se $b \neq 0, e\ a.b = 0$, então $a.b = 0.b$ e pela lei do cancelamento da multiplicação, $a = 0$.

Logo, sempre que um fator for não nulo, o outro será, necessariamente, nulo.

■

**Subtração em $\mathbb{Z}$**

Dados $a$ e $b$ pertencentes a $\mathbb{Z}$, definimos a diferença $a - b$ por

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

Note que "subtrair" é "somar o oposto".

Assim, a **subtração** em $\mathbb{Z}$ é uma função que associa cada par $(a, b)$ ao número $a + (-b)$, ou seja:

$$- : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$$
$$(a, b) \mapsto a + (-b)$$

A subtração não é associativa, nem comutativa, nem tem elemento neutro.

## 2.2.2 Proposições em $\mathbb{Z}$

Os resultados a seguir, que chamaremos "proposições", decorrem das operações e das propriedades já demonstradas.

**Proposição 1.** *Para todos* $a,b$ *inteiros tem-se que* $(a-b)+b=a$.

**Demonstração.**

Hipótese: $a,b$ são números inteiros

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

Sejam a e b inteiros. Pela definição de subtração temos que

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

Mas $[a+(-b)]+b=a+[(-b)+b]$ pela propriedade associativa da adição; assim, $a+[(-b)+b]=a+0=a$ (propriedade do oposto e propriedade do elemento neutro da adição). Logo $(a-b)+b=a$.

■

**Proposição 2.** *O oposto da soma de dois inteiros é igual à soma dos opostos dos dois inteiros. Ou seja, se* $a$ *e* $b$ *são números inteiros,*

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

**Demonstração.**

Para provar uma igualdade, uma estratégia é sair de um membro da igualdade e chegar ao outro membro, por meio de deduções lógicas e fazendo uso de resultados teóricos. Aplicaremos esta estratégia nesta demonstração.

Hipótese: $a$ *e* $b$ são números inteiros.

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

De fato, usando propriedades já conhecidas temos que:

$$-(a+b)=(-1).(a+b)=(-1).a+(-1).b=(-a)+(-b).$$

(na primeira igualdade usamos P3, na segunda igualdade usamos a propriedade distributiva e, na terceira, usamos novamente P3).

■

**Proposição 3.** *O oposto do produto de dois números inteiros é igual a um dos números multiplicado pelo oposto do outro. Ou seja:*

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

Faremos a demonstração em duas partes: primeiramente mostraremos que (-a) b = -(ab) e depois que a(-b) = -(ab); com isto teremos provado a igualdade -(ab) = (-a)b = a(-b).

**Demonstração.**

Mostremos que $(-a).b = -(a.b)$. De fato,

$$(-a).b = [(-1).a].b = (-1).(a.b) = -(ab).$$

Na primeira e terceira igualdades usamos P3 e, na segunda igualdade, usamos a propriedade associativa da multiplicação.

De forma análoga, prova-se que : $a.(-b) = -(a.b)$.

Assim, temos que: $(-a).b = a.(-b) = -(a.b)$.

■

**Proposição 4.** *O oposto do oposto de um número inteiro é o próprio número ou seja,* $-(-a) = a$ .

**Demonstração.**

Hipótese: $a$ é um número inteiro.

Tese: $-(-a) = a$ .

De fato. Seja $a$ um número inteiro. Sabemos que o oposto de $-a$ é o único inteiro $x$ que satisfaz a equação $-a + x = 0$. Como $-a + a = 0$, segue que o oposto de $-a$ *é* $a$, ou seja, $-(-a) = a$ .

■

**Exemplos:** Seja $a$ um número inteiro qualquer.

- se $a$ é maior do que zero, o oposto de $a, -a$, é menor do que zero; ou seja: $-a$ é um inteiro negativo.
- se $a$ é menor do que zero, o oposto de $a, -a$, é maior do que zero; ou seja: $-a$ é um inteiro positivo.

Vejamos sobre a reta numérica:

1) se $a > 0$,


2) se $a < 0$,

**Por exemplo:** Se $a = -2$, temos que $-2 + 2 = 0$. Logo o oposto de $-2$ *é* $2$, ou seja, $-(-2) = 2$.

**Proposição 5.** *O produto do oposto de* $a$ *pelo oposto de* $b$ *é o produto* $a.b$.

**Demonstração.**

Hipótese: $a$ *e* $b$ são inteiros, $-a$ é o oposto de $a$ e $(-b)$ é o oposto de $b$.

Tese: $(-a).(-b) = a.b$.

Usando a proposição 3 duas vezes consecutivas temos que:

$$(-a).(-b) = -[a.(-b)] = -(-ab).$$

Mas, pela proposição 4, $-(-ab) = a.b$. Logo, $(-a).(-b) = a.b$.

■

Estabelecido P4 como axioma, pode-se provar a "lei do cancelamento para a multiplicação em $\mathbb{Z}$". Agora já temos elementos para efetivar essa demonstração.

**Proposição 6.** *Sejam* $a, b$ e $c$ *inteiros e* $c \neq 0$. *Se* $a.c = b.c$ *então* $a = b$.

**Demonstração.**

Hipótese: $a, b, c$ inteiros, $ac = bc$ e $c \neq 0$, $ac = bc$.

Tese: $a = b$.

Sejam $a, b$ e $c$ inteiros tais que $ac = bc$ *e* $c \neq 0$; queremos provar que $a = b$. De fato, somando aos dois membros da igualdade $ac = bc$ o termo $(-bc)$, temos:

$$ac + (-bc) = bc + (-bc).$$

Como $bc + (-bc) = 0$, podemos escrever

$$ac + (-bc) = bc + (-bc) = 0.$$

Pela proposição 3, temos que $(-bc) = (-b).c$; substituindo esse resultado na igualdade acima e usando a propriedade distributiva obtemos $[a + (-b)]c = 0$; como $c \neq 0$, segue por P4 que $a + (-b) = 0$. Então $a = -(-b) = b$. Pela proposição 4, $a = b$.

■

**Proposição 7.** *O oposto de* $a-b$ *é* $b-a$, *ou seja,* $-(a-b)=b-a$.

**Demonstração.**

Hipótese: $a$ *e* $b$ são números inteiros.

Tese: $-(a-b)=b-a$.

De fato,

$$(a-b)+(b-a)=[a+(-b)]+[b+(-a)]=$$

$$=a+[(-b)+b]+(-a)=a+0+(-a)=a+(-a)=0.$$

Logo, pela propriedade do oposto, segue que o oposto de $(a-b)$ *é* $(b-a)$, ou seja,

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

■

**Proposição 8.** *Para todos* $a,b$ *e* $c$ *pertencentes a* $\mathbb{Z}$, $a.(b-c)=ab-ac$.

**Demonstração.**

De fato:

$$a.(b-c)=a[b+(-c)]=a.b+a.(-c)=ab+(-ac)=ab-ac.$$

■

Na primeira igualdade, usamos a definição de subtração, na segunda igualdade, usamos a propriedade distributiva, na terceira igualdade, usamos a Proposição 3 e, na quarta igualdade, usamos a definição de subtração.

## Exercício proposto

2) Resolva a equação seguinte, explicando cada passo

$$x+45=3x-7.$$

## 2.2.3 Relação de ordem em $\mathbb{Z}$

Vamos retomar os subconjuntos de $\mathbb{Z}$:

- $\mathbb{Z}_+=\{0,1,2,3,4,5,\ldots\}$, inteiros não negativos ($\mathbb{N}$).
- $\mathbb{Z}_+^*=\mathbb{Z}_+-\{0\}$, inteiros positivos.

- $\mathbb{Z}_- = \{0, -1, -2, -3, -4, -5, \ldots\}$, inteiros não positivos.
- $\mathbb{Z}_-^* = \mathbb{Z}_- - \{0\}$, inteiros negativos.

**Relação de ordem "menor ou igual" em $\mathbb{Z}$**

**Definição.** Dados $a$ e $b$ inteiros, dizemos que "$a$ *é menor ou igual a* $b$", se e somente se $(b-a)$ pertence a $\mathbb{Z}_+$.

Em linguagem simbólica escrevemos:

$$a \leq b \Leftrightarrow (b-a) \in \mathbb{Z}_+ .$$

**Observação 1.** Pode-se ler também: "$b$ *é maior ou igual a* $a$" e denota-se por $b \geq a$.

Habitualmente usamos a expressão "menor ou igual a" mas a expressão gramaticamente correta seria "menor do que ou igual a".

**Observação 2.** "$a$ é menor ou igual a $b$", se e somente se existe $x \in \mathbb{Z}_+$ tal que $b = a + x$.

De fato, tomemos $x = (b-a) \in \mathbb{Z}_+$. Então,

$$a + x = a + (b-a) = a + [b + (-a)] = b + [a + (-a)] = b + 0 = b .$$

Reciprocamente, se existe $x \in \mathbb{Z}_+$ tal que $b = a + x$, teremos que $x = (b-a) \in \mathbb{Z}_+$. Por definição, teremos $a \leq b$.

**Propriedades da relação "$\leq$" em $\mathbb{Z}$**

Sejam $a, b$ e $c \in \mathbb{Z}$.

O1) **Propriedade Reflexiva:** Para todo $a \in \mathbb{Z}$ tem-se $a \leq a$.

**Demonstração.**

Hipótese: $a \in \mathbb{Z}$.

Tese: $a \leq a$.

De fato, $a - a = 0 \in \mathbb{Z}_+ \Leftrightarrow a \leq a$.

■

O2) **Propriedade anti-simétrica:** Para todos $a,b \in \mathbb{Z}$, *se* $a \leq b$ *e* $b \leq a$ *então* $a = b$.

**Demonstração.**

Hipótese: $a,b \in \mathbb{Z}$, $a \leq b$ *e* $b \leq a$.

Tese: $a = b$.

Por hipótese, temos que:

i) $a \leq b \Leftrightarrow b - a \in \mathbb{Z}_+$

ii) $b \leq a \Leftrightarrow a - b \in \mathbb{Z}_+$

Sabemos que $-(a-b)+(a-b)=0$ (Proposição 7) e que $a-b$ e seu oposto estão em $\mathbb{Z}_+$ (hipótese). Pela lei do anulamento isto só acontece se $a-b=0$, donde (pela definição de subtração) $a+(-b)=0$. Somando $b$ em ambos os membros da igualdade temos que $a+(-b)+b=0+b$ e, aplicando as propriedades do elemento neutro da adição e do elemento oposto, obtemos $a+0=b$. Portanto: $a=b$.

■

O3) **Propriedade transitiva:** Para todos $a,b$ *e* $c \in \mathbb{Z}$, *se* $a \leq b$ *e* $b \leq c$ *então* $a \leq c$.

**Demonstração.**

Hipótese: $a,b$ *e* $c \in \mathbb{Z}$; $a \leq b$ *e* $b \leq c$.

Tese: $a \leq c$.

De fato: Por hipótese:

$a \leq b \Leftrightarrow b - a \in \mathbb{Z}_+$

$b \leq c \Leftrightarrow c - b \in \mathbb{Z}_+$.

Logo: $(b-a)+(c-b) \in \mathbb{Z}_+$, portanto:

$$c - a = c - a + (b - b) = [b + (-a)] + [c + (-b)] = [(b-a)+(c-b)] \in \mathbb{Z}_+$$

donde, por definição de "menor ou igual", temos $a \leq c$.

■

As propriedades reflexiva, anti-simétrica e transitiva caracterizam a relação "$\leq$" como uma relação de ordem em $\mathbb{Z}$.

**Definição.** Sejam $a$ e $b$ inteiros. Dizemos que "$a$ *é menor do que* $b$" ou que "$b$ *é maior do que* $a$" se e somente se $b-a \in \mathbb{Z}_+^*$. Em linguagem simbólica:

$$a < b \Leftrightarrow b-a \in \mathbb{Z}_+^* \text{ e } b > a \Leftrightarrow b-a \in \mathbb{Z}_+^*.$$

**Observações importantes:** Considerando $a$ um número inteiro, temos:

1) $a > 0 \Leftrightarrow 0 < a \Leftrightarrow a-0 \in \mathbb{Z}_+^* \Leftrightarrow -(-a) \in \mathbb{Z}_+^* \Leftrightarrow$
$\Leftrightarrow 0+[-(-a)] \in \mathbb{Z}_+^* \Leftrightarrow 0-(-a) \in \mathbb{Z}_+^* \Leftrightarrow -(-a) \in \mathbb{Z}_+^* \Leftrightarrow -a < 0$

   Ou seja, $-a \in \mathbb{Z}_-^*$

2) $a < 0 \Leftrightarrow a = -(-a) < 0 \overset{Por\ 1}{\Leftrightarrow} -a > 0.$

**Proposição 9.** *Sejam* $a, b$ *e* $c$ *números inteiros. Então*

i) $a \le b \Leftrightarrow a+c \le b+c$, *para todo* $c \in \mathbb{Z}$

ii) $a \le b$ *e* $c > 0$ *então* $ac \le bc$

iii) $a \le b$ *e* $c \le 0$ *então* $bc \le ac$.

**Demonstração de (i).**

Por hipótese, $a \le b \Leftrightarrow b-a \in \mathbb{Z}_+$. Agora notemos que:

$$(b+c)-(a+c) = b+c+[-(a+c)] = (b+c)+(-a)+(-c) = [b+(-a)]+[c+(-c)] =$$
$$= (b-a)+0 = (b-a) \in \mathbb{Z}_+$$

Assim, $b+c \ge a+c$.

Reciprocamente se $(b+c)-(a+c) \in \mathbb{Z}_+$ e como $(b+c)-(a+c) = b-a$, temos que $(b-a) \in \mathbb{Z}_+$. Logo $a \le b$.

■

**Demonstração de (ii).**

Por hipótese $a \le b$ *e* $c \ge 0$; *então* $b-a \in \mathbb{Z}_+$ *e* $c \in \mathbb{Z}_+$.

Logo, $bc-ac = (b-a).c \in \mathbb{Z}_+$ (pois o produto de dois números naturais resulta um número natural) e portanto $ac \le bc$.

■

**Demonstração de (iii).**

Por hipótese, se $a \leq b$ *então* $b-a \in \mathbb{Z}_+$. Como $c \leq 0$ tem-se que $c \in \mathbb{Z}_-$, $-c \in \mathbb{Z}_+$

Logo $(b-a).(-c) = b(-c) - a(-c) \in \mathbb{Z}_+$. Assim, usando as propriedade convenientes temos: $-bc + ac \in \mathbb{Z}_+$, ou seja,

$$ac - bc \in \mathbb{Z}_+ .$$

Portanto, $bc \leq ac$.

■

**Proposição 10.** *Sejam a e b números inteiros.*
*Se* $a \leq b$ *então* $(-b) \leq (-a)$.

**Demonstração.**

Sejam $a$ *e* $b$ inteiros tais que $a \leq b$; somando $-b$ em ambos os membros da desigualdade temos:

$a + (-b) \leq b + (-b)$.

Assim, $a + (-b) \leq 0$. Somando $-a$ em ambos os membros desta última desigualdade temos $-a + a + (-b) \leq 0 + (-a)$. Como $-a + a = 0$, *e* $0 + (-a) = -a$, podemos concluir:

$$(-b) \leq (-a).$$

■

**Proposição 11.** *(Regra de sinais) Sejam* $a$ *e* $b$ *números inteiros. Então,*

i) *Se* $a \leq 0$ *e* $0 \leq b$ *então* $ab \leq 0$

ii) *Se* $a \leq 0$ *e* $b \leq 0$ *então* $ab \geq 0$

**Demonstração de (i).**

*Se* $a \leq 0$ *e* $0 \leq b$ *então* $a \in \mathbb{Z}_-$ *e* $b \in \mathbb{Z}_+$; também $(-a) \in \mathbb{Z}_+$.

Logo $(-a)b \in \mathbb{Z}_+$ *e* $-(ab) \in \mathbb{Z}_+$. Pela propriedade do elemento neutro da adição temos:

$0 + [-(ab)] = 0 - ab \in \mathbb{Z}_+$. Portanto $ab \leq 0$.

■

**Demonstração de (ii).**

*Se* $a \leq 0$ *e* $b \leq 0$ *então* $0-a \in \mathbb{Z}_+$ *e* $0-b \in \mathbb{Z}_+$; assim, $-a \in \mathbb{Z}_+$ *e* $-b \in \mathbb{Z}_+$. Portanto $(-a).(-b) \in \mathbb{Z}_+$ *e* $a.b \in \mathbb{Z}_+$. Logo, $0 \leq a.b$.

■

**Observação:** Se $a \geq 0$ *e* $b \geq 0$, ou seja, se $a$ *e* $b \in \mathbb{Z}_+$ então $a$ *e* $b$ pertencem a $\mathbb{N}$; mas $\mathbb{N}$ é fechado em relação à multiplicação, isto é, o produto de quaisquer dois números naturais é um número natural. Então $ab \geq 0$.

**Proposição 12.** *(Lei da tricotomia) Dado* $a \in \mathbb{Z}$, *uma e somente uma das opções ocorre:*

i) $a > 0$ ou

ii) $a = 0$ ou

iii) $a < 0$ (ou exclusivo).

**Proposição 13.** *Sejam* $a$, $b$ *e* $c$ *números inteiros. Se* $a \leq b$ *e* $c \leq d$ *então* $a + c \leq b + d$.

**Demonstração.** Faça como exercício.

## Exercício proposto

3) Resolva a inequação seguinte, explicando cada passo:

$$2x - 22 \leq 3x + 7.$$

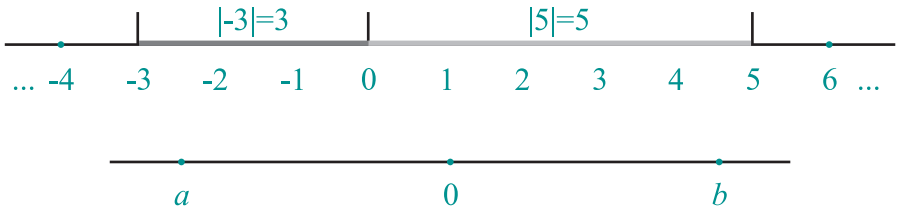
## 2.2.4 Valor absoluto em $\mathbb{Z}$

**Definição.** Seja $a \in \mathbb{Z}$. Definimos o valor absoluto de $a$, ou módulo de $a$, como:

$$|a| = \begin{cases} a \text{ se } 0 \leq a \quad \text{e} \\ -a \text{ se } a < 0 \end{cases}$$

**Por exemplo:** $|-17| = -(-17)$, *pois* $-17 < 0$; $|157| = 157$, *pois* $157 > 0$.

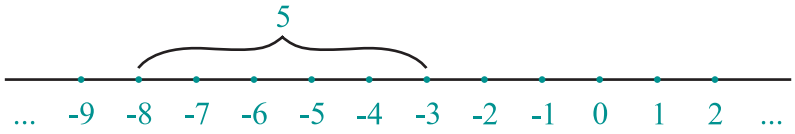
**Observação 1.** o valor absoluto de um número inteiro é a distância dele até a origem.




Para $a$ e $b$ como acima temos $|b| = b$ e $|a| = -a$.

**Observação 2.** $|a-b|$ é a distância de $a$ até $b$. Exemplos:

$$|3-5| = |-2| = 2;\ |-8-(-3)| = |-5| = 5;\ |2-(-1)| = 3$$




**Propriedades do valor absoluto**

**Propriedade 1.** $0 \le |a|$, para todo $a \in \mathbb{Z}$; também $|a| = 0 \Leftrightarrow a = 0$.

**Demonstração.**

Se $0 \le a$ temos que, então $0 \le a = |a|$. Também, temos que,

$$|a| = 0 \Leftrightarrow a = 0 \ ou\ -a = 0 \Leftrightarrow a = 0.$$

Se $a < 0$, $|a| = -a$. Pela proposição 9, item (iii), se $a < 0$ então $-a > 0$. Portanto, $|a| = -a > 0$.

■

**Propriedade 2.** Para todo $a$ inteiro, tem-se $|a| = |-a|$.

**Demonstração.**

Se $0 \le a$ temos por definição que $|a| = a$; além disso, $-a \le 0$. Assim, $|-a| = -(-a) = a$. Portanto, $|a| = a = |-a|$.

Se $a < 0$, temos que $|a| = -a$ e $0 \le -a$; portanto, $|-a| = -a$. Assim, $|a| = -a = |-a|$.

■

**Propriedade 3.** Para todo $a$ inteiro tem-se $-|a| \le a \le |a|$.

**Demonstração.**

Se $0 \le a$ então, $|a| = a \ge 0$. Multiplicando por $(-1)$, $|a| = a \ge 0$, obtemos que

$-|a| = -a \leq 0$. Portanto, $-|a| = -a \leq 0 \leq a = |a|$, ou seja, $-|a| \leq 0 \leq |a|$.

Se $a < 0$, então $|a| = -a,\ 0 < -a,\ e\ -|a| = a$. Portanto

$$-|a| = a < 0 < -a = |a|.$$

■

**Propriedade 4.** $|a.b| = |a|.|b|$, para todos $a\ e\ b$ inteiros.

**Demonstração.**

Se $a \geq 0,\ b \geq 0$ então $ab \geq 0$. Logo $|ab| = ab = |a|.|b|$

Se $a \geq 0,\ b \leq 0,\ |a| = a,\ |b| = -b\ e\ ab \leq 0$.

Assim, $|a|.|b| = a.(-b) = -(ab)$. Mas,

$|a.b| = -(ab)$. Portanto: $|a.b| = |a|.|b|$.

Se $a \leq 0,\ b \leq 0$ temos $|a| = -a.\ |b| = -b\ e\ 0 \leq ab$.

Também $|a|.\ |b| = (-a).(-b) = ab$.

Mas, $|ab| = ab$. Logo $|ab| = |a|.|b|$.

■

**Propriedade 5 (Desigualdade triangular).** $|a+b| \leq |a| + |b|$, para todos $a\ e\ b$ inteiros.

**Demonstração.**

Observemos que $a \leq |a|$ e $b \leq |b|$; logo, pela Proposição 13, $a + b \leq |a| + |b|$. De forma análoga, temos que $(-a) + (-b) \leq |-a| + |-b|$. Agora, consideremos dois casos:

i) Se $(a+b) < 0$ então

$$|a+b| = -(a+b) = -a + (-b) \leq |-a| + |-b| = |a| + |b|.$$

A última igualdade segue da Propriedade 2 de valor absoluto.

ii) Se $(a+b) > 0$ então $|a+b| = a + b \leq |a| + |b|$.

Portanto por i) e ii) temos que: $|a+b| \leq |a| + |b|$.

■

Agora que já conhecemos as operações e principais propriedades dos conjuntos dos números naturais e inteiros, vamos conhecer mais uma característica de cada um destes conjuntos.

## 2.2.5 Princípio da Boa ordem em $\mathbb{N}$

O que é este princípio?

O princípio da boa ordem afirma que: "Todo subconjunto não vazio de números naturais possui um menor elemento".

Ou ainda, se S é um subconjunto não vazio de $\mathbb{N}$, então S tem um menor elemento.

**Exemplo:** Considere os subconjuntos de $\mathbb{N}$, $A \subset \mathbb{N}$, $B \subset \mathbb{N}$ *e* $C \subset \mathbb{N}$**:**

$$A = \{2, 3, 4, \ldots\}$$

$$B = \{8, 12, 16, 20\}$$

$$C = \{215, 315, 415, 515, \ldots\}$$

- O menor elemento de $A$ *é* $2$.
- O menor elemento de $B$ *é* $8$.
- O menor elemento de $C$ *é* $215$.

**Definição.** Dizemos que $a$ é o menor elemento de um subconjunto não vazio S de $\mathbb{N}$ quando para todo $b$ pertencente a S, tem-se que $a$ é menor ou igual a $b$.

As duas proposições abaixo são conseqüências do Princípio da Boa Ordem (PBO):

**Proposição 14.** *Se* $a \in \mathbb{N}$ *e* $0 \leq a \leq 1$, *então* $a = 0$ *ou* $a = 1$.

**Demonstração.**

Vamos fazer a demonstração por contradição. Suponhamos que exista um número inteiro $a$ diferente de zero e diferente de um nestas condições, isto é, $0 \leq a \leq 1$. Então o conjunto $S = \{x \in \mathbb{Z} : 0 < x < 1\}$ é não vazio e é um subconjunto de $\mathbb{N}$. Pelo PBO existe $m \in S$ tal que $m$ é o menor elemento de $S$, ou seja, $m \leq x$ para todo $x \in S$. Como $m \in S$, temos que $m > 0$ *e* $m < 1$.

Multiplicando ambos os membros da última desigualdade por $m$, temos $m.m < 1.m$, isto é, $0 < m^2 < m$. Como $m < 1$, podemos escrever:

$0 < m^2 < m < 1$, e daí $0 < m^2 < 1$. Mas, se ocorre esta desigualdade, podemos concluir que $m^2 \in S$.

Assim, $m^2 \in S$ *e* $m^2 < m$, sendo $m$ o menor elemento de $S$! Isto é uma contradição pois $m$ é estritamente menor do que todo elemento de $S$. Logo, como nossa suposição levou-nos a uma contradição, o fato que havíamos suposto não pode ocorrer. Isto significa que não é possível existir um número inteiro $a$ tal que $0 < a < 1$. Assim, se ocorrer $0 \leq a \leq 1$ deve necessariamente ocorrer a igualdade, ou seja, $a = 0$ *ou* $a = 1$.

■

**Proposição 15.** *Se* $a, b \in \mathbb{N}^*$, *existe* $n \in \mathbb{N}^*$ *tal que* $na > b$.

**Exemplo:** Note que se $a > b$, qualquer $n$ serve; o mesmo acontece se $a = b$. Vejamos um exemplo para $a < b$.

Se $a = 2$ *e* $b = 7$, existe um $n = 4$ tal que $2.4 = 8 > 7$.

Note que $n$ não é único.

**Demonstração da Proposição 15.**

Hipótese: $a, b \in \mathbb{N}^*$.

Tese: existe $n \in \mathbb{N}^*$ tal que $na > b$.

Sejam $a$ *e* $b \in \mathbb{N}^*$; devemos exibir um número natural $n$ tal que $na > b$.

De fato: seja $S = \{m \in \mathbb{N}^* : ma > b\}$. Note que $S \neq \varnothing$, pois $(b+1) \in S$ desde que

$$(b+1)a = (ba + a) > b.$$

Logo, pelo Princípio da Boa Ordem, existe um $n \in S$ tal que $n \leq x$ para todo $x \in S$.

Ou seja, existe $n \in \mathbb{N}^*$ tal que $na > b$ *e* $n \leq m$ para todo $m \in \mathbb{N}^*$ tal que $ma > b$.

Conseguimos assim exibir um número $n$ que satisfaz $na > b$.

■

## 2.2.6 Princípio do Menor Inteiro em $\mathbb{Z}$ (PMI)

Para enunciar o PMI em $\mathbb{Z}$ vamos precisar de algumas definições:

**Definição.** (conjunto limitado inferiormente) Seja $A$ um subconjunto de números inteiros. Dizemos que $A$ é *limitado inferiormente* quando existe um inteiro $k$, tal que $k \leq a$ para todo $a$ pertencente a $A$.

**Definição.** (elemento mínimo) Seja $a_0$ um elemento pertencente ao conjunto $A$. Dizemos que $a_0$ *é mínimo de* $A$ quando $a_0 \leq a$, para todo $a \in A$.

Denotamos o mínimo de $A$ por $\min A = a_0$.

Pode-se provar que o elemento mínimo é único.

**Princípio do Menor Inteiro em** $\mathbb{Z}$: Se $A \subset \mathbb{Z}$, $A \neq \varnothing$ e $A$ é limitado inferiormente, então $A$ possui **mínimo**.

**Conseqüências:**

1) $a-1$ é o maior inteiro menor do que $a$, para todo $a \in \mathbb{Z}$.

2) Para todos $a, b \in \mathbb{Z}$, se $a \leq b \leq a+1$, então $b = a$ *ou* $b = a+1$.

O primeiro resultado mostra que, no conjunto dos números inteiros, é possível identificar qual o maior número menor que um número dado. Por exemplo, para $a = 78$, $a-1 = 77$ é o número "mais próximo" de $78$ e menor do que ele. Outra conseqüência deste resultado é que, se $a$ *e* $b$ são inteiros e $a < b$, então $a \leq b-1$. O segundo resultado mostra que entre dois inteiros consecutivos não há número inteiro algum; por exemplo, não há inteiros entre $54$ e seu sucessor, $54+1=55$.

## Exercícios propostos

4) Explique qual propriedade ou definição foi usada em cada passagem da demonstração abaixo: "Para todos $a, b$ *e* $c$ inteiros tem-se: $a(b-c) = ab - ac$".

**Demonstração.**

$$a.(b-c) = a.[b+(-c)] = a.b + a.(-c) = a.b + [-(a.c)] = ab - ac.$$

5) Determine um número natural que, quando multiplicado por $21$, resulta um número formado apenas com algarismos $4$.

6) Seja $A$ um subconjunto limitado inferiormente, e não vazio de $\mathbb{N}$. Mostre que o menor elemento de $A$ é único.

7) Mostre que: Para todos $a,b$ pertencentes a $\mathbb{N}$, se $a \leq b \leq a+1$, então $b=a$ ou $b=a+1$. (Sugestão: Use a Proposição 14 )

8) Prove a Proposição 13: *Se* $x<y$ *e* $z<t$ *então* $x+z<y+t$.

9) Prove que se $0<a\leq b$ *e* $0<x<y$ *então* $0<ax<by$.

# Resumo

Neste capítulo, apresentamos os conjuntos dos números naturais e dos números inteiros (chamados conjuntos numéricos), bem como as operações de adição e multiplicação em $\mathbb{N}$ com as respectivas propriedades: associativa, comutativa, elemento neutro, cancelamento e anulamento.

Também discutimos a subtração e a divisão em $\mathbb{N}$. Vimos que a diferença, $a-b$ está definida em $\mathbb{N}$ quando $a \geq b$. A divisão em $\mathbb{N}$, $a \div b$ está definida se $b$ é um divisor de $a$.

Também definimos a Relação "menor ou igual" em $\mathbb{N}$. Mostramos que a relação "menor ou igual", em $\mathbb{N}$, define uma relação de ordem, isto é, satisfaz as propriedades: reflexiva, anti-simétrica e transitiva.

Estudamos o "Princípio da boa ordem" em $\mathbb{N}$: "Todo subconjunto não vazio de números naturais possui um menor elemento".

Similarmente, em $\mathbb{Z}$, estudamos as operações de adição, multiplicação e subtração e suas propriedades; para a adição: associativa, comutativa, elemento neutro e elemento oposto. As propriedades da multiplicação estudadas foram: associativa, comutativa e elemento neutro. Estudamos, também, a propriedade distributiva, relacionada às duas operações.

Ainda estudamos a relação "menor ou igual", em $\mathbb{Z}$. Mostramos que a relação "menor ou igual" em $\mathbb{Z}$ define uma relação de ordem, isto é, satisfaz as propriedades: reflexiva, anti-simétrica e transitiva.

Também estudamos a definição de valor absoluto e suas propriedades; e outras proposições importantes em $\mathbb{N}$, e em $\mathbb{Z}$. Finalizando estudamos o "Princípio do Menor Inteiro" em $\mathbb{Z}$: "Se $A \subset \mathbb{Z}$, $A \neq \varnothing$ e $A$ limitado inferiormente, então $A$ possui elemento mínimo".

## Bibliografia comentada

DOMINGUES, Hygino H. **Fundamentos de Aritmética**. São Paulo: Atual, 1991.

Este livro é ótima referência como bibliografia básica. Trata do conteúdo estudado neste capítulo com muita clareza e propriedade, além de propor exercícios variados.

# Capítulo 3

## Divisibilidade e Algoritmo da Divisão

# Capítulo 3

## Divisibilidade e Algoritmo da Divisão

*Neste capítulo, desenvolveremos o conceito de divisibilidade em $\mathbb{N}$ e em $\mathbb{Z}$, apresentando os elementos necessários à compreensão e utilização do principal teorema relacionado a este conceito: o Algoritmo da Divisão. Em seguida faremos um estudo das conseqüências deste resultado: máximo divisor comum, equações diofantinas, mínimo múltiplo comum e congruências.*

Os nossos objetos de estudo, neste capítulo, não são assuntos novos; certamente você já conhece divisores e múltiplos em $\mathbb{N}$ e a fatoração de um número natural em produto de primos (conteúdos de 5ª e 6ª séries do ensino fundamental). Historicamente, os livros VII, VIII e IX dos Elementos de Euclides (c. 300 a.C.) tratam exatamente de aritmética teórica, apresentando os conceitos de divisor, múltiplo, número primo, algoritmo para cálculo do máximo divisor comum e outros conceitos e resultados utilizados até hoje. Para os gregos deste período, um número era um segmento, ou seja, um "comprimento". A definição 5 do livro VII dos Elementos ilustra bem esta idéia quando apresenta o conceito de divisor da seguinte forma:

"Um número é parte de outro, o menor do maior, quando ele mede o maior".

A palavra "parte" pode ser substituída por "divisor" e "medir o maior" significa que este maior número é igual a um número inteiro de vezes o menor número. Em outras palavras, é a definição de divisor em $\mathbb{N}$.

Neste capítulo, vamos um pouco além de Euclides, estendendo o conceito de divisibilidade ao conjunto dos números inteiros, com todas as conseqüências. O Algoritmo da Divisão será apresentado em $\mathbb{N}$ e em $\mathbb{Z}$ e demonstrado em $\mathbb{Z}$. O estudo do máximo divisor

comum e do mínimo múltiplo comum será feito inicialmente em $\mathbb{N}$ e depois será estendido para $\mathbb{Z}$. As congruências módulo $n$, uma conseqüência da divisibilidade, serão estudadas em $\mathbb{Z}$. Sugerimos que você comece o estudo com lápis e papel na mão, e tenha sempre em mente que o que você estudou no capítulo 2 será amplamente utilizado neste capítulo e o que estudará neste capítulo, será amplamente utilizado no próximo!

## 3.1 Divisibilidade em $\mathbb{N}$ e em $\mathbb{Z}$

Nosso estudo de divisibilidade será no conjunto dos números inteiros; faremos a comparação com as definições e resultados no conjunto $\mathbb{N}$ sempre que algum fato diferente ocorrer na transição de $\mathbb{N}$ para $\mathbb{Z}$. Começamos com as definições abaixo, apresentadas nos dois conjuntos. Como você pode notar, a definição de divisor em $\mathbb{N}$ se estende de modo natural aos números inteiros. Caso não seja especificado o conjunto, você deve considerar $\mathbb{Z}$ como universo de trabalho.

**Definição 1.** Divisibilidade em $\mathbb{N}$

Sejam $a$ e $b$ números naturais. Dizemos que $a$ é *divisor* de $b$ se, e somente se, existe um número natural $n$ tal que $b = a.n$.

**Definição 2.** Divisibilidade em $\mathbb{Z}$

Sejam $a$ e $b$ números inteiros. Dizemos que $a$ é *divisor* de $b$ se, e somente se, existe um número inteiro $n$ tal que $b = a.n$.

**Exemplos**

1) $48$ é um divisor de $144$ pois existe um número inteiro $n = 3$ tal que $144 = 48.3$.

2) $-7$ é um divisor de $35$ pois existe um número inteiro $n = -5$ tal que $35 = (-7).(-5)$.

3) $31$ é um divisor de $-62$ pois existe um número inteiro $n = -2$ tal que $-62 = 31.(-2)$.

4) $-15$ é um divisor de $-60$ pois existe um número inteiro $n = 4$ tal que $-60 = (-15).4$.

**Notação.** Para $a$ e $b$ inteiros, "$a$ é divisor de $b$" será anotado por $a|b$; note que o traço é vertical e **não indica** uma fração. A propósito, ainda não conhecemos frações! Nosso universo de trabalho é o conjunto dos números inteiros. Nos exemplos acima, anotamos: $48|144;\ (-7)|35;\ 31|(-62);\ (-15)|(-60)$. Quando $a$ *não é divisor de* $b$ anotamos $a \nmid b$; por exemplo, $4 \nmid 50$.

Simbolicamente, escrevemos: $(\forall a, b \in \mathbb{Z})\ (a \mid b \Leftrightarrow \exists n \in \mathbb{Z} : b = a.n)$.

*Sobre o uso de símbolos, note que:*

1) Os símbolos que indicam os quantificadores $\forall$ (qualquer que seja, para todo, para cada etc.) e $\exists$ (existe pelo menos um) serão utilizados a partir de agora, assim como a notação das sentenças condicionais e bicondicionais. Você pode consultar seu material de primeiro semestre para revisar este assunto. Utilizaremos também o símbolo $\in$, que representa a pertinência de um elemento a um conjunto; por exemplo, escrevemos $x \in \mathbb{Z}$ para indicar que $x$ é um número inteiro. Para indicar que um elemento não pertence a um conjunto A escreve-se $x \notin \mathbb{Z}$; por exemplo, $-5 \notin \mathbb{N}$.

**Taquigrafia**
*sf (taqui+grafo[1]+ia[1])* Arte de escrever tão depressa como se fala por meio de sinais e abreviaturas; estenografia.
*Fonte: www2.uol.com.br/michaelis/*

2) O uso de símbolos para escrever matemática é bastante conveniente, mas exige um certo cuidado. Primeiro, lembrar sempre que o símbolo *representa* uma idéia; não é uma espécie de taquigrafia para escrever mais rápido! Segundo, lembrar sempre que não podemos "misturar" símbolos e linguagem corrente na mesma sentença; isto vale inclusive para os símbolos dos conjuntos numéricos $\mathbb{N}$ e $\mathbb{Z}$. Vamos dar alguns exemplos:

   a) $(\forall a \in \mathbb{Z})(\exists b \in \mathbb{Z})(a + b = 0)$

      Representa a sentença "Para todo número inteiro $a$ existe um número inteiro $b$ tal que a adição de $a$ com $b$ é igual a zero" (Axioma da existência do oposto em $\mathbb{Z}$, capítulo 2).

   b) $(\exists x \in \mathbb{Z})(\forall b \in \mathbb{Z})(b + x = b)$

      Representa a sentença "Existe um número inteiro $x$ tal que para qualquer número inteiro $b$, a adição de $b$ com $x$ é igual a $b$." (Axioma da existência do elemento neutro da adição em $\mathbb{Z}$, no capítulo 2).

**Observação 1.** Quando um inteiro $a$ é divisor de um inteiro $b$, isto é, existe $n \in \mathbb{Z}$ tal que $b = a.n$, o inteiro $n$ também será um divisor de $b$; por exemplo, $3$ é divisor de $45$ pois $45 = 3.15$ e $15$ é também um divisor de $45$. Assim, quando identificamos um divisor de um número inteiro, estamos, na verdade, identificando dois deles (que eventualmente podem ser iguais, como no caso $36 = 6.6$).

**Observação 2.** Quando $a$ é divisor de $b$ podemos expressar este fato de várias formas:

| $a$ é divisor de $b$ pode ser expresso por | Exemplo: 15 é divisor de 60 |
|---|---|
| (i) $a$ é divisor de $b$ | 15 é divisor de 60 |
| (ii) $b$ é divisível por $a$ | 60 é divisível por 15 |
| (iii) $a$ divide $b$ | 15 divide 60 |
| (iv) $b$ é múltiplo de $a$ | 60 é múltiplo de 15 |

Em (i) temos a definição 3.1.2. Em (ii) temos a expressão "ser divisível", utilizada no ensino fundamental: $100$ é divisível por $10$ (pois $100 = 10.10$), $46$ é divisível por $23$ (pois $46 = 23.2$).

A expressão em (iii) dispensa o uso do verbo "ser" e usa o verbo "dividir"; é bastante utilizada em livros.

A última linha do quadro (expressão (iv)) usa o conceito de múltiplo de um número inteiro:

"Sejam $x$ *e* $y$ inteiros; dizemos de $x$ é múltiplo de $y$ se e somente se existe um número inteiro $n$ tal que $x = y.n$". Desta forma, as expressões "$a$ é divisor de $b$" e "$b$ é múltiplo de $a$" são sinônimos.

**Observação 3.** Observe a definição de divisor:

$$(\forall a, b \in \mathbb{Z})\ (a \mid b \Leftrightarrow \exists n \in \mathbb{Z} / b = a.n).$$

O que podemos dizer se $a$ *ou* $b$ for igual a zero?

i) se $b = 0$ *e* $a \neq 0$, existe $n = 0 \in \mathbb{Z}$ tal que $0 = a.0$ e teremos que $a$ é divisor de $b = 0$. Logo, $a \mid 0$, para todo $a \neq 0$. Por exemplo, $5$ é divisor de $0$ pois existe $n = 0$ tal que $0 = 5.0$.

ii) se $b \neq 0$ *e* $a = 0$, não é possível encontrar $n \in \mathbb{Z}$ tal que $b = 0.n$, ou seja, $b \neq 0.n$, para todo $n$ inteiro. Logo, $0 \nmid b$, para todo $b \neq 0$. (Lembre que o produto de um número inteiro por zero resulta sempre zero. Resultado do capítulo 2: "Para todo inteiro a tem-se $a.0 = 0$").

iii) se $a = 0$ *e* $b = 0$, para qualquer número inteiro $n$ teremos $0 = n.0$; assim $0 \mid 0$.

Podemos concluir, então, que o único caso em que o zero pode assumir o papel de divisor é o caso (iii), quando $a = b = 0$. Por este motivo, a partir de agora, estaremos considerando sempre divisores não nulos, ou seja, quando escrevermos "$a$ é divisor de $b$", você pode considerar $a \neq 0$.

**Observação 4.** É importante lembrar que quando dizemos $a \mid b$, não estamos nos referindo à *operação divisão*, que não está definida em $\mathbb{Z}$. A divisibilidade é uma *relação* entre inteiros: dados dois inteiros $x$ *e* $y$, ou $x$ é divisor de $y$ ou não é. Você terá oportunidade de estudar com detalhes a teoria e as aplicações das relações na disciplina de Introdução ao Cálculo.

**Propriedades da divisibilidade**

As propriedades que apresentamos a seguir são instrumentos essenciais para o desenvolvimento dos próximos capítulos. Observe que as demonstrações utilizam os axiomas e propriedades estudados no capítulo 2; procure identificá-los. De modo geral, após o enunciado de cada propriedade, identificaremos "hipótese" e "tese" antes de iniciarmos a demonstração. Não usaremos, ainda, a linguagem simbólica, para que você se familiarize com as idéias.

Nas propriedades que seguem, consideraremos *a, b* e *c* números inteiros.

D1) *Para todo* $a$ *inteiro tem-se que a é divisor de* $a$.

**Demonstração.**

Como $a = a.1$ (Axioma da existência do elemento neutro da multiplicação em $\mathbb{Z}$) para todo $a$ inteiro, temos que $a$ é divisor de $a$.

■

D2) *Se $a$ é divisor de $b$ e $b$ é divisor de $c$ então $a$ é divisor de $c$.*

**Demonstração.**

Hipótese: $a$ é divisor de $b$ e $b$ é divisor de $c$.

Tese. $a$ é divisor de $c$.

Para provarmos que $a$ é divisor de $c$, devemos mostrar que $c = a.x$, para algum $x$ inteiro; em outras palavras, devemos exibir um inteiro $x$ que satisfaça a igualdade

$$c = a.x .$$

Por hipótese, temos que $a$ é divisor de $b$ e $b$ é divisor de $c$; isto significa que existem inteiros $n$ e $m$ tais que $b = a.n$ (1) e $c = b.m$ (2). Substituindo (1) em (2) temos

$$c = (a.n).m = a.(n.m) .$$

Desta forma, encontramos um inteiro $x = n.m$ que nos permite escrever $c = a.x$; por definição, temos que $a$ é divisor de $c$.

■

D3) *Se $a$ é divisor de $b$ e $b$ é divisor de $a$ então $a = b$ ou $a = -b$.*

**Demonstração.**

Hipótese: $a$ é divisor de $b$ e $b$ é divisor de $a$.

Tese: $a = b$ ou $a = -b$.

Por hipótese, temos que existem inteiros $s$ ou $t$ tais que $b = a.s$ (1) e $a = b.t$ (2). Substituindo (1) em (2) temos $a.1 = (a.s).t = a.(s.t)$; como $a \neq 0$ (Obs.3) podemos cancelá-lo e teremos $1 = s.t$.

Mas, quais são os inteiros cujo produto é 1? As únicas possibilidades para $s$ e $t$ são:

$$s = t = 1 \text{ ou } s = t = -1 .$$

Assim, substituindo $s$ e $t$ nas igualdades (1) e (2) teremos $a = b$ ou $a = -b$, como queríamos provar.

■

D4) *Se $a$ é divisor de $b$ então $a$ é divisor de $kb$, para todo $k$ inteiro.*

**Demonstração.**

Hipótese: $a$ é divisor de $b$.

Tese: $a$ é divisor de $bk$, para todo $k$ inteiro.

Por hipótese, temos que existe $n$ inteiro tal que $b = a.n$; multiplicando ambos os membros da igualdade por um inteiro $k$ qualquer obtemos $b.k = (a.n).k = a.(n.k)$, ou seja, $a$ é divisor de $bk$.

■

**Observação 5.** A propriedade 4 nos diz que, se um número é divisor de outro, será também divisor de qualquer múltiplo deste outro. Por exemplo, como $3$ é divisor de $6$, $3$ será divisor de todos os múltiplos de $6: 12, 18, 24, -12, -36$ etc. O conjunto dos múltiplos de um número inteiro $b$ pode ser expresso por:

$$M_b = \{bk / k \in \mathbb{Z}\} = \{0, b, 2b, 3b, 4b, \ldots, -b, (-2)b, (-3)b, \ldots\}.$$

D5) *Se $a$ é divisor de $b$ e $a$ é divisor de $c$ então $a$ é divisor de $(b+c)$ e $a$ é divisor de $(b-c)$.*

**Demonstração.**

Hipótese: $a \mid b$ e $a \mid c$.

Tese: $a \mid (b+c)$ e $a \mid (b-c)$.

Provaremos que $a$ é divisor de $(b+c)$; faça a prova de $a \mid (b-c)$ como exercício.

Por hipótese, temos que existem inteiros $m$ e $n$ tais que $b = a.n$ e $c = a.m$; somando membro a membro as igualdades, obtemos: $b + c = a.n + a.m = a.(n+m)$. Logo, $a$ é divisor de $(b+c)$.

■

D6) *Se $a$ é divisor de $(b+c)$ e $a$ é divisor de $b$ então $a$ é divisor de $c$.*

**Demonstração.**

Hipótese: $a$ é divisor de $(b+c)$ e $a$ é divisor de $b$.

Tese: $a$ é divisor de $c$.

Por hipótese, temos que existem $x$ e $y$ inteiros tais que $b+c=a.x$ e $b=a.y$. Substituindo o valor de $b$ na primeira igualdade obtemos:

$$(a.y)+c=a.x$$
$$c=a.x-a.y$$
$$c=a(x-y)$$

Logo, temos que $a$ é divisor de $c$.

■

D7) *Se $a$ é divisor de $b$ e $b\neq 0$ então $|a|\leq|b|$.*

**Demonstração.**

Hipótese: $a$ é divisor de $b$ e $b\neq 0$.

Tese: $|a|\leq|b|$.

Por hipótese, existe um inteiro $n$ tal que $b=a.n$, e $b\neq 0$. Então $|b|=|a.n|=|a|.|n|$.

Como $|a|.|n|\neq 0$ e $|n|$ é um inteiro positivo, teremos que $|b|=|a|.|n|\geq|a|$, como queríamos provar.

■

## Exercícios resolvidos

1) Um número divisível por $2$ é chamado um número *par*. Mostre que a soma e o produto de dois números pares é também um número par.

**Resolução.** Sejam $x$ e $y$ números pares, ou seja, ambos são divisíveis por $2$. Pela definição de divisibilidade, existem inteiros $n$ e $m$ tais que $x=2.n$ e $y=2.m$. Observemos a soma e o produto de $x$ e $y$:

$x+y=2.n+2.m=2.(n+m)$ é divisível por $2$ e

$x.y=(2.n).(2.m)=2.(2.n.m)$ é também divisível por $2$.

Logo, a soma e o produto de dois números pares é também um número par.

(Identifique, na resolução anterior, os resultados do capítulo $2$ que foram utilizados na resolução!)

2) Mostre que, se um número $n$ é divisível por $15$, então ele também é divisível por $5$.

**Resolução.** Se $n$ é divisível por $15$, então existe um inteiro $k$ tal que $n = 15.k$.

Como $15 = 3.5$, podemos escrever $n = (3.5).k = (5.3).k = 5.(3.k)$ que é divisível por $5$.

## Exercícios propostos

1) Se um número inteiro é divisor de um produto, podemos afirmar que ele é também divisor dos fatores? Justifique.

2) Se um número inteiro é divisor de uma soma, podemos afirmar que ele é também divisor das parcelas? Justifique.

# 3.2 Algoritmo da Divisão em $\mathbb{N}$ e em $\mathbb{Z}$

O Algoritmo da Divisão (também conhecido como algoritmo de Euclides) aparece nos *Elementos* de Euclides (c.300 a.C.) como um teorema. Ele é um velho conhecido até das crianças: corresponde à nossa conhecida "conta de dividir", que aprendemos nas séries iniciais do ensino fundamental, ainda no universo dos números naturais. Por exemplo, a divisão de $182$ por $12$:

$$\begin{array}{r|l} 182 & 12 \\ \cline{2-2} 62 & 15 \\ 2 & \end{array}$$

Vamos recordar a terminologia: $182$ é o *dividendo*; $12$ é o *divisor*; $15$ é o *quociente* e $2$ é o *resto*. Sabemos também que:

1) é possível verificar se a conta está correta verificando se ocorre a igualdade:

$$\text{dividendo} = (\text{divisor}).(\text{quociente}) + \text{resto}$$

Em nosso exemplo, $182 = 12.15 + 2$.

2) o resto deve ser sempre *menor* do que o divisor; se o resto for maior, ou estamos errando na subtração, ou o quociente é maior. Diferente dos algoritmos da multiplicação e adição, o

algoritmo da divisão exige que se faça uma estimativa do quociente: quantos "12" cabem em 182?

**Teorema 1. Algoritmo da Divisão em $\mathbb{N}$**

Sejam $a$ e $b$ números naturais com $b \neq 0$; então existe um único par de números naturais $q$ e $r$ de modo que $a = b \cdot q + r$, com $0 \leq r < b$.

**Observação 6.** O teorema 1 nos garante que dados $a$ e $b$ (com $b$ diferente de 0) é sempre possível encontrar números $q$ e $r$ satisfazendo a condição $a = b.q + r$, com $0 \leq r < b$.

Vejamos alguns exemplos:

1) Se $a = 7$ *e* $b = 4$, existem $q = 1$ *e* $r = 3$ tais que $7 = 4.1 + 3$ *e* $3 < 4$.
2) Se $a = 5$ *e* $b = 13$, procuramos $q$ *e* $r$ tais que $5 = 13.q + r$; como $q$ *e* $r$ são naturais, devemos ter $q = 0$ *e* $r = 5 < 13$, ou seja, $5 = 13.0 + 5$.
3) Se $a = 0$ *e* $b = 17$, para que se tenha $0 = 17.q + r$, devemos ter necessariamente $q = r = 0$.

**Observação 7.** A idéia central do Algoritmo da Divisão é que, dados dois números $a$ e $b$ (com $b \neq 0$), temos somente duas possibilidades: $a$ é múltiplo de $b$ ou $a$ está entre dois múltiplos de $b$. Ou seja: $a = b.q$ *ou* $b.q < a < b.(q+1)$. Veja na reta:


Sabendo disso, para encontrar o quociente devemos nos fazer a seguinte pergunta: qual o múltiplo de $b$ mais próximo de $a$ e menor do que $a$? Vejamos alguns exemplos:

1) para $a = 43$ *e* $b = 5$

   Qual o múltiplo de 5 mais próximo de 43 e menor do que 43?

Este múltiplo é $40 = 5.8$ e "faltam" $3$ unidades para "chegar" ao $43$. Temos então $q = 8$ *e* $r = 3$, ou seja, $43 = 5.8 + 3$.

2) para $a = 114$, $b = 7$.

Qual o múltiplo de $7$ mais próximo de $114$ e menor do que $114$? Neste ponto você sugere: faça a conta!!

$$\begin{array}{r|l} 114 & 7 \\ \cline{2-2} 44 & 16 \\ 2 & \end{array}$$

A conta, como a conhecemos, é o Algoritmo da divisão repetido várias vezes. Observe que ao fazermos "11 dividido por 7" no primeiro passo da conta, já estamos utilizando o Algoritmo da divisão e, na verdade, separar o $11$ é uma maneira mais rápida de estimar o quociente, a partir da centena $110$. Veja a conta na horizontal, com o Algoritmo da divisão utilizado várias vezes:

$$11 = 7.1 + 4.$$

Como estamos estimando para centena, multiplicamos ambos os membros por 10:

$$11.10 = (7.1 + 4).10$$
$$110 = 7.10 + 40.$$

Como queremos $114$, somamos $4$ a ambos os membros:

$$110 + 4 = 7.10 + 40 + 4$$
$$114 = 7.10 + 44.$$

Aplicando o AD para $44$ e $7$, obtemos $44 = 7.6 + 2$; substituindo, temos:

$$114 = 7.10 + 7.6 + 2$$
$$114 = 7.(10 + 6) + 2$$
$$114 = 7.16 + 2.$$

Vemos, assim, que o múltiplo de $7$ mais próximo de $114$ é $7.16$ e está $2$ unidades à esquerda de $114$: $q = 16$ *e* $r = 2$. Concluímos, então, que o "procedimento" da conta de dividir em $\mathbb{N}$ é o Algoritmo da divisão aplicado repetidas vezes, aliado às propriedades das operações de adição e multiplicação em $\mathbb{N}$.

Se pensarmos no Algoritmo da divisão como uma forma de relacionar números, ou seja, dado um par de números $a$ e $b$, encontrar um par $q$ e $r$ satisfazendo determinadas condições, podemos nos perguntar: é possível estendermos esta idéia ao conjunto dos números inteiros? A resposta é sim, com uma modificação.

**Teorema 2. Algoritmo da Divisão em $\mathbb{Z}$**

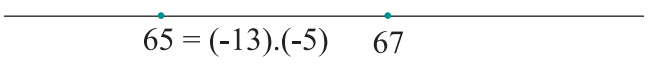
Sejam $a$ e $b$ números inteiros com $b \neq 0$; então existe um único par de números inteiros $q$ e $r$ de modo que $a = b \,.\, q + r$, com $0 \leq r < |b|$.

A diferença entre o Algoritmo da divisão em $\mathbb{N}$ e em $\mathbb{Z}$ aparece na condição $0 \leq r \leq |b|$, indicando que o resto deverá ser sempre um número positivo. A idéia permanece a mesma: encontrar o múltiplo de $b$ mais próximo de $a$ e menor do que ele.

**Exemplos**

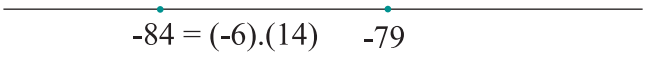
1) Se $a = -55$ e $b = 4$, o múltiplo de $4$ mais próximo de $-55$ e menor do que ele é $4.(-14) = -56$ e a distância entre $-55$ e $-56$ é de uma unidade. Assim, o quociente é $-14$ e o resto é $1 : -55 = 4.(-14) + 1$. Veja na reta:


2) Se $a = 67$ e $b = -5$, o múltiplo de $-5$ mais próximo de $67$ e menor do que ele é $(-5).(-13) = 65$ e a distância entre $67$ e $65$ é de $2$ unidades. Assim teremos o quociente $q = -13$ e o resto $r = 2$; $67 = (-13).(-5) + 2$.




Note que, mesmo quando o divisor é negativo, permanece a mesma idéia: procurar o múltiplo de $-5$ mais próximo de $67$ e menor do que $67$.

3) Se $a = -79$ *e* $b = -6$, o múltiplo de $-6$ mais próximo de $-79$ e menor do que ele é $(-6).14 = -84$ e a distância entre $-79$ *e* $-84$ é de $5$ unidades. Isto nos dá o quociente $q = 14$ e o resto $r = 5 : -79 = (-6).14 + 5$




**Observação 8.** Note que o Algoritmo da Divisão em $\mathbb{Z}$ não corresponde à "conta de dividir", exceto quando o resto é zero!

**Demonstração do Algoritmo da Divisão em $\mathbb{Z}$**

Faremos a demonstração inicialmente para $a \in \mathbb{Z}_+$ *e* $b \in \mathbb{Z}_+^*$ $(b \neq 0)$, ou seja, $a \geq 0$ *e* $b > 0$; em seguida para $a < 0$ *e* $b > 0$ e por fim para $b < 0$ e $a$ qualquer.

- **1º caso:** $a \geq 0$ *e* $b > 0$

Devemos mostrar a existência e a unicidade dos números $q$ *e* $r$. Faremos separadamente: primeiro demonstraremos a existência e depois a unicidade.

**i) Existência**

Considere o conjunto $S = \{a - b.x \geq 0 \,/\, x \in \mathbb{Z}\}$.

Note que $S$ é o conjunto das diferenças $a - b.x$, construído com valores de $x$ que satisfazem $a - b.x \geq 0$ $(ou,\ b.x \leq a)$. Observe também que:

1) $S \subset \mathbb{N}$, pois os elementos de $S$ são maiores ou iguais a zero.

2) $S \neq \varnothing$, pois para $x = 0$ a diferença $a - b.0 = a$ é um elemento do conjunto $S$, uma vez que $b.0 = 0 \leq a$ pois $a \in \mathbb{Z}_+$.

"Todo subconjunto não vazio de números naturais possui um menor elemento"

Pelo Princípio da Boa Ordenação em $\mathbb{N}$ podemos concluir que $S$ possui um *menor* elemento $r$, satisfazendo:

i) $r \in S$

ii) $r \leq s$, para todo $s \in S$

Este menor elemento é o número $r$ (o resto) que estamos procu-

rando. De fato, como $r \in S$, este elemento $r$ é uma "diferença", ou seja, existe um $q \in \mathbb{Z}$ tal que $r = a - b.q \geq 0$. Isto significa que $a = b.q + r$ *e* $r \geq 0$. Ainda resta provar que $r < b$. (Note que eliminamos o módulo pois $b \in \mathbb{Z}_+^*$).

Para provar este fato, vamos supor (por contradição) que $r \geq b$. A que isto nos leva? Observe o que acontece quando fazemos uma diferença com o sucessor de $q$, $q+1$:

$$a - b.(q+1) = a - b.q - b = (a - b.q) - b = r - b \geq 0,$$

pois estamos supondo $r \geq b$. Então

$$a - b.(q+1) \in S \text{ e } a - b.(q+1) = r - b < r.$$

Isto é uma contradição pois $r$ é o *menor* elemento do conjunto $S$; a suposição $r \geq b$ nos levou a um elemento do conjunto $S$.

Este elemento de $S$ é a diferença $a - b.(q+1)$, que é menor do que $r$, quando $r$ é o *menor* dos elementos de $S$!

Logo, não pode ocorrer $r \geq b$, o que significa que $0 \leq r < b$. Assim, provamos a existência de $q$ *e* $r$ inteiros tais que $a = b.q + r$, *e* $0 \leq r < b$.

**ii) Unicidade**

Provamos que dados $a, b \in \mathbb{Z}_+^*$, existem $q, r \in \mathbb{Z}_+$ tais que $a = b.q + r$, com $0 \leq r < b$.

Para provar que $q$ *e* $r$ são únicos, suponhamos que existam $s$ *e* $t$ inteiros, $s, t \in \mathbb{Z}_+^*$, tais que $a = b.s + t$, com $0 \leq t < b$. A **unicidade** será provada se mostrarmos que $q = s$ *e* $r = t$.

De modo geral, para provarmos que um número que satisfaz uma condição é único, supomos que existe outro número satisfazendo a condição e provamos que eles devem ser iguais.

Temos então duas igualdades:

$$a = b.q + r, \text{ com } 0 \leq r < b \text{ e } a = b.s + t, \text{ com } 0 \leq t < b$$

e podemos escrever

$$b.q + r = b.s + t$$
$$b.q - b.s = t - r$$
$$b(q - s) = t - r.$$

Esta última igualdade nos mostra que $b|(t-r)$; se $t-r \geq 0$, pela propriedade D7, temos $b < |t-r|$. Como $0 \leq r < b$ *e* $0 \leq t < b$, concluímos que a distância entre $t$ *e* $r$ é menor do que $b$, ou seja, $0 \leq |t-r| < b$. Assim, se $t-r \neq 0$, temos duas conclusões contraditórias: $b < |t-r|$ *e* $|t-r| < b$. Isto significa que não pode ocorrer $t-r \neq 0$, ou seja, devemos ter $t-r=0$, *ou* $t=r$. Substituindo esta informação na igualdade $b.(q-s)=t-r$, obtemos $b.(q-s)=0$. Como $b \neq 0$ por hipótese, devemos ter $q-s=0$, ou seja, $q=s$.

Provamos assim que, dados $a \in \mathbb{Z}_+$ *e* $b \in \mathbb{Z}_+^*$, só existe *um par de números* $q$ *e* $r$ satisfazendo as condições: $a=b.q+r$ *e* $0 \leq r < b$.

- **2º caso:** $a<0$ *e* $b>0$

Sabemos que $|a|<0$; logo, pelo 1º caso, temos que existem $q'$ *e* $r' \in \mathbb{Z}_+^*$ tais que $|a|=b.q'+r'$, com $0 \leq r' < b$. Vamos analisar os casos $r'=0$ *e* $r'>0$:

a) Se $r'=0$, teremos $|a|=b.q'$; como $|a|=-a$, podemos escrever $-a=b.q'$ e conseqüentemente $a=b.(-q')$. Logo, existem $q=-q'$ *e* $r=0$ tal que $a=b.q+r$.

b) Se $r'>0$, teremos

$$a=-|a|=-(b.q'+r')=b.(-q')-r'=$$

$$=b.(-q')+b-b-r'=b.(-q'-1)+(b-r').$$

Observando a igualdade acima, vemos que se $a=b.(-q'-1)+(b-r')$ (Note que como $r'<b$ tem-se $b-r'>0$) encontramos $q=-q'-1$ *e* $r=b-r'$, tais que $a=b.q+r$ e $0 \leq r < b$.

- **3º caso:** $b<0$ e $a$ qualquer

Para quaisquer $a$ *e* $|b|$, existem $q', r' \in \mathbb{Z}$ tais que $a=|b|.q'+r'$, com $0 \leq r' < |b|$.

(Lembre que o 1º caso garante a existência de $q$ *e* $r$ para $a \geq 0$ *e* $b>0$ e o 2º caso garante a existência de $q$ *e* $r$ para $a<0$ *e* $b>0$.)

Como $|b|=-b$, temos: $a=(-b).q'+r'=b.(-q')+r'$. Logo, existem $q=-q'$ *e* $r=r'$ inteiros tais que $a=b.q+r$, com $0 \leq r < |b|$.

Deixamos como exercício a prova da unicidade nos casos 2 e 3.

**Observação 9.** Sobre a demonstração do Algoritmo da Divisão.

A demonstração do Algoritmo da Divisão nos dá a receita de como encontrar $q$ *e* $r$ satisfazendo as condições $a = b.q + r$, com $0 \leq r < |b|$. Vamos seguir os passos da demonstração com um exemplo numérico. Sejam $a = 57$ *e* $b = 12$ (Note que esta é a situação do 1º caso da demonstração). Construímos o conjunto $S$ para $a = 57$ *e* $b = 12$; os elementos do conjunto $S$ são as diferenças $57 - 12x$ que são maiores ou iguais a zero, quando $x$ percorre o conjunto dos números inteiros. Assim, $S$ pode ser escrito como $S = \{57 - 12x \geq 0 / x \in \mathbb{Z}\}$. Os valores de $x$ que tornam a diferença $57 - 12x$ maior ou igual a zero são $x = 1, 2, 3$ *ou* $4$; assim, o conjunto $S$ será dado por

$$S = \{(57 - 12.1), (57 - 12.2), (57 - 12.3), (57 - 12.4)\} = \{45, 33, 21, 9\}.$$

O resto $r$ será o menor elemento do conjunto $S$, ou seja, $r = 9$. A diferença que resulta $r = 9$ *é* $9 = 57 - 12.4$, ou ainda $57 = 12.4 + 9$. Encontramos assim $q = 4$ *e* $r = 9$, satisfazendo as condições. Veja que, ao tomar $r$ como o mínimo do conjunto $S$, estamos procurando "o múltiplo de 12 *mais próximo* de 57 e menor do que ele", situação já ilustrada nos exemplos iniciais.

Para valores negativos de $a$ *ou* $b$ (ou ambos), o procedimento também está descrito na demonstração. Vejamos alguns exemplos:

- **2º caso:** Para $a = -50$ *e* $b = 6$ usamos o procedimento do 1º caso para $|-50| = 50$ *e* $6$: existem $q' = 8$ *e* $r' = 2$ tais que $50 = 6.8 + 2$. Fazendo $q = (-q') - 1 = (-8) - 1 = -9$ e $r = b - r' = 6 - 2 = 4$, obtemos $-50 = 6.(-9) + 4$, com $0 \leq r < 6$.
- **3º caso:** Para $a = 76$ *e* $b = -13$ usamos o procedimento do 1º caso para $76$ *e* $|-13| = 13$ e encontramos $q' = 5$ *e* $r' = 11$ tais que $76 = 13.5 + 11$. Fazendo $q = -q' = -5$ *e* $r = r' = 11$, obtemos $76 = (-13).(-5) + 11$. O quociente é $-5$ e o resto é 11.

No caso de $a$ *e* $b$ negativos, por exemplo, $a = -83$ *e* $b = -11$, fazemos o procedimento para $a = (-83)$ *e* $b = |-11| = 11$ e encontramos $q' = -8$ *e* $r' = 5$ tais que $-83 = 11.(-8) + 5$. Fazendo $q = -q' = 8$ *e* $r = r' = 5$ obtemos $-83 = (-11).8 + 5$. O quociente é $8$ e o resto é $5$.

**Observação 10.** Já comentamos que o Algoritmo da Divisão em $\mathbb{Z}$ não corresponde à "conta de dividir", como ocorria em $\mathbb{N}$; queremos dizer com isso que o Algoritmo da Divisão não se configura como uma *operação* em $\mathbb{Z}$, mas como uma *relação* entre inteiros. Por este motivo, o Algoritmo da Divisão é conhecido como "divisão euclidiana": encontrar quociente e resto da divisão euclidiana de dois inteiros $a$ e $b$ corresponde a encontrar $q$ e $r$ inteiros tais que $a = b.q + r$, com $0 \leq r < |b|$.

## 3.3 Consequências do Algoritmo da Divisão

1) Quando para dois inteiros $a$ e $b$ temos quociente $q$ e resto zero, ou seja, $a = b.q + 0$, concluímos que $b|a$. Assim, podemos dizer que $b|a$ quando o resto da divisão euclidiana de $a$ por $b$ é zero.

2) A limitação do resto pelo módulo do divisor na divisão euclidiana nos fornece uma espécie de "classificação" dos inteiros, em relação a um divisor. Vejamos alguns exemplos:

   a) para o divisor $b = 2$, os possíveis restos da divisão euclidiana são $0$ *ou* $1$, uma vez que para qualquer inteiro $a$ tem-se $a = 2.q + r$ e $0 \leq r < 2$. Isto significa que para qualquer inteiro $a$, temos duas possibilidades, e somente uma das duas ocorre: $a = 2.q + 0$ *ou* $a = 2.q + 1$. Este fato estabelece duas classes já conhecidas de números inteiros:

   - os inteiros *pares*, da forma $a = 2.q$.
   - os inteiros *ímpares*, da forma $a = 2.q + 1$.

   b) para o divisor $b = 3$, os possíveis restos da divisão euclidiana são 0, 1 ou 2, pois para qualquer inteiro a tem-se $a = 3.q + r$, com $0 \leq r < 3$. Podemos então estabelecer três classes de inteiros:

   - aqueles que na divisão euclidiana por 3 têm resto zero: $a = 3.q + 0$, ou seja, são divisíveis por 3.
   - aqueles que na divisão euclidiana por 3 têm resto 1: $a = 3.q + 1$.

- aqueles que na divisão euclidiana por $3$ têm resto $2$: $a = 3.q + 2$.

Podemos, assim, construir três conjuntos de inteiros, cada um correspondendo a um resto na divisão por $3$:

- resto $0$, conjunto $A = \{\ldots, -6, -3, 0, 3, 6, 9, \ldots\}$
- resto $1$, conjunto $B = \{\ldots, -5, -2, 1, 4, 7, 10, \ldots\}$
- resto $2$, conjunto $C = \{\ldots, -4, -1, 2, 5, 8, 11, \ldots\}$.

Note que não há elementos comuns nestes conjuntos: eles são **disjuntos**, dado qualquer inteiro $x$, ele pertence a apenas um dos três conjuntos $A$, $B$ *ou* $C$.

Dois conjuntos são disjuntos quando não possuem elementos comuns.

c) Generalizando as idéias anteriores, podemos dizer que dado um inteiro $b \neq 0$, todo inteiro $n$ pode ser expresso de uma, e somente uma das formas:

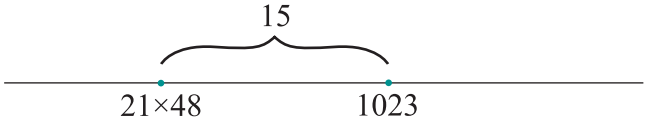
$$\begin{gathered} n = b.q \ ou \\ n = b.q + 1 \ ou \\ n = b.q + 2 \ ou \\ \vdots \\ n = b.q + (b-1). \end{gathered}$$

Cada expressão depende do resto da divisão euclidiana de $n$ por $b$; o conjunto dos possíveis restos será $M = \{0, 1, 2, \ldots, b-1\}$, caracterizando a segunda parcela de cada expressão.

## Exercícios resolvidos

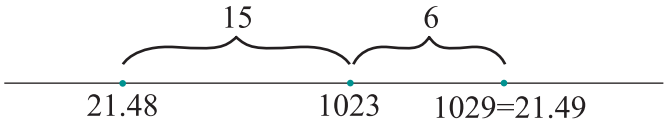
3) Determine o menor número natural de $4$ algarismos diferentes que seja divisível por $21$.

**Resolução.** O menor número natural de $4$ algarismos diferentes é $1023$; aplicando o Algoritmo da Divisão para $1023$ *e* $21$ obtemos $1023 = 21.48 + 15$. Isto significa que o maior múltiplo de $21$ que é menor do que $1023$ é $21.48 = 1008$. Veja na reta:



Como $1023$ é o *menor* número de quatro algarismos diferentes, devemos procurar o menor múltiplo de $21$ *maior* do que $1023$ (na reta, o que está mais próximo de $1023$, à sua direita). Como $1008 = 21.48$, tomamos o próximo múltiplo de $21$, ou seja, $21.49 = 1029$. Como $1029$ tem algarismos diferentes, encontramos nossa resposta. Caso encontrássemos um número com algarismos repetidos, tomaríamos entre os múltiplos maiores do que $1008$, o primeiro múltiplo de $21$ que satisfizesse as condições.

Note que conhecido o resto $15$ da divisão euclidiana de $1023$ por $21$, outra maneira de resolver seria somar $6$ (pois $15+6=21$) a $1023$, ou seja, somar o que falta a $1023$ para termos o próximo múltiplo de $21$. Veja na reta:




**Resposta.** O menor número de quatro algarismos diferentes que é múltiplo de $21$ é $1029$.

4) Determine todos os possíveis números naturais que na divisão euclidiana por $7$ têm o quociente igual ao dobro do resto.

**Resolução.** Seja $n$ a representação dos números procurados; o problema nos informa que, ao aplicarmos o Algoritmo da Divisão para $n$ e $7$, obtemos $q$ e $r$ tais que $n = 7.q + r$, com $q = 2.r$ e $0 \le r < 7$. Logo, $n = 7.(2r) + r = 14.r + r = 15.r$, com $0 \le r < 7$. Esta última desigualdade nos informa que os possíveis valores de $r$ são 0, 1, 2, 3, 4, 5 ou 6; para cada um deles vamos encontrar um valor de $n$, como mostra a tabela:

| $r$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| $n = 15.r$ | 0 | 15 | 30 | 45 | 60 | 75 | 90 |

Faça a verificação da resposta do problema sempre que possível; isto fará com que você possa corrigir eventuais erros, dando-lhe autonomia para "validar" a resposta. Torne-se independente do "gabarito"!

**Resposta.** Os números procurados são $0, 15, 30, 45, 60, 75$ e $90$.

**Observação.** Você pode verificar se resolveu corretamente o problema fazendo a divisão euclidiana dos valores encontrados por $7$ e observando se o quociente é o dobro do resto. Por exemplo, $60 = 7.8 + 4$, $r = 4$ e $q = 8 = 2.4$.

5) Quais são os números de dois algarismos que divididos pela soma de seus algarismos resulta quociente $4$ e resto zero?

**Resolução.** Os números de dois algarismos são da forma $n = 10a + b$, com $b$ variando de $0$ $a$ $9$ e $a$ variando de $1$ $a$ $9$. O problema nos informa que $n = 4.(a+b)+0$, ou seja,

$$10a + b = 4a + 4b$$
$$10a + (-4a) = 4b + (-b)$$
$$6a = 3b$$
$$3.2.a = 3.1.b$$
$$2a = b\,.$$

Esta igualdade nos fornece uma relação entre os algarismos $a$ e $b$. Vejamos agora as possibilidades para $a$ e $b$ que vão gerar os números procurados:

| $a$ | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| $b = 2.a$ | 2 | 4 | 6 | 8 | 10 não é um algarismo! |
| $n = 10a + b$ | $10.1+2=12$ | $10.2+4=24$ | $10.3+6=36$ | $10.4+8=48$ | |
| Teste | $12 = 4.(1+2)$ | $24 = 4.(2+4)$ | $36 = 4.(3+6)$ | $48 = 4.(4+8)$ | |

**Resposta.** Os números são $12$, $24$, $36$ *e* $48$.

## Exercícios propostos

3) Determine o maior número natural de $5$ algarismos diferentes que seja divisível por $17$.

4) a) Mostre que a soma e produto de números pares é um número par.

b) Mostre que a soma de um número par com um número ímpar é um número ímpar.

5) Mostre que um número inteiro formado por três algarismos iguais é sempre múltiplo de $37$.

6) Determine todos os números naturais $n$ tais que na divisão euclidiana de $n$ por $12$ o resto excede o quociente em $7$ unidades.

# 3.4 Máximo Divisor Comum e Mínimo Múltiplo Comum

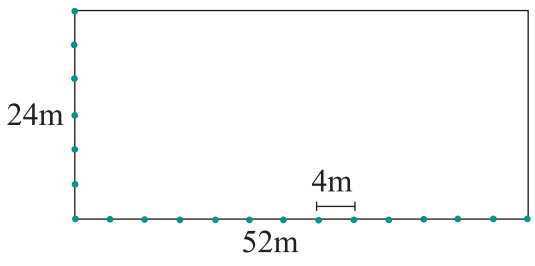
Os conceitos de *máximo divisor comum* e *mínimo múltiplo comum* ocupam um papel importante na estrutura do conjunto dos números inteiros e são muito úteis na resolução de problemas. Estas idéias serão generalizadas mais tarde (na disciplina de Álgebra) em outros conjuntos, servindo de base para a construção de novas estruturas algébricas. No Ensino Fundamental, estes conceitos já são estudados; no entanto, são utilizados durante toda vida escolar, uma vez que os conjuntos numéricos e suas propriedades constituem uma ferramenta de trabalho poderosa no estudo de todos os conteúdos do Ensino Fundamental e do Ensino Médio. Faremos nosso estudo inicialmente no conjunto dos números naturais, estendendo-o em seguida para o conjunto dos números inteiros.

## 3.4.1 Máximo divisor comum (mdc)

Considere o seguinte problema:

"Um terreno retangular de 52 m por 24 m será cercado. Em toda volta desse cercado serão plantados arbustos igualmente espaçados. Qual o maior espaço possível entre os arbustos?"

Trata-se, aqui, de encontrar um número que divida igualmente as dimensões do terreno, $52$ *e* $24$, e seja o maior deles. Em outras palavras, encontrar o maior número que seja divisor de $52$ *e* $24$ simultaneamente. Os divisores de $24$ são $1, 2, 3, 4, 6, 8, 12$ *e* $24$. Os divisores de $52$ são $1, 2, 4, 13, 26$ *e* $52$. Os divisores comuns são 1, 2 e 4. O maior deles é $4$. Logo, podemos dividir as dimensões do terreno por $4$ e teremos espaços iguais em toda a volta. Veja o desenho.



A resposta do problema é: o maior espaço possível entre os arbustos é 4 m.

O que fizemos foi calcular o *máximo divisor comum* dos números 24 e 52. Vamos ver a definição formal de máximo divisor comum:

**Definição.** Sejam $a$ e $b$ números naturais, não nulos simultaneamente. Um número natural $d$ é o máximo divisor de $a$ e $b$ se, e somente se, são satisfeitas as condições:

i) $d$ é divisor de $a$ e $d$ é divisor de $b$;

ii) se $k$ é um divisor de $a$ e $k$ é um divisor de $b$, então $k$ é divisor de $d$.

**Notação**. Quando $d$ é o máximo divisor comum dos números $a$ e $b$, anotamos $d = mdc(a,b)$.

**Observação 11.** A primeira condição da definição nos informa que para ser o máximo divisor comum dos números $a$ e $b$, $d$ deve ser um divisor comum; a segunda nos informa que $d$ deve ser o maior deles, ou seja, se existir outro divisor comum de $a$ e $b$, ele deverá ser também um divisor de $d$. Como $d$ é um *divisor*, ele será um número estritamente maior do que zero ($d > 0$).

**Exemplos**

1) $mdc(36,24) = 12$ pois:
divisores de 36: 1, 2, 3, 4, 6, 9, **12**, 18 *e* 36
divisores de 24: 1, 2, 3, 4, 6, 8, **12** *e* 24
**12** é o máximo divisor comum de 36 *e* 24.

2) $mdc(21,15) = 3$ pois:
divisores de 21: 1, **3**, 7 *e* 21
divisores de 15: 1, **3**, 5 *e* 15
**3** é o máximo divisor comum de 21 *e* 15.

3) $mdc(16,35) = 1$ pois:
divisores de 16: **1**, 2, 4, 8 *e* 16
divisores de 35: **1**, 5, 7 *e* 35
**1** é o máximo divisor comum de 16 *e* 35.

**Observação 12.** Note que a ordem em que os números aparecem não é relevante; assim, $mdc(a,b) = mdc(b,a)$.

## 3.4.2 Propriedades do mdc em $\mathbb{N}$

P1) Se $a$ é um número natural não nulo, então $mdc(a,0) = a$.

**Demonstração.**

Hipótese: $a \in \mathbb{N}$ *e* $a \neq 0$.

Tese: $mdc(a,0) = a$.

Mostremos que o número $a$ satisfaz as duas condições da definição:

i) $a \mid a$ *e* $a \mid 0$ pois $a = a.1$ *e* $0 = a.0$.

ii) se $k$ é um número natural tal que $k \mid a$ *e* $k \mid 0$, então, podemos concluir que $k \mid a$.

Logo, $mdc(a,0) = a$.

■

P2) Sejam $a$ *e* $b$ números naturais não nulos simultaneamente. Se $a \mid b$ então $mdc(a,b) = a$.

**Demonstração.**

Hipótese: $a,b \in \mathbb{N}^*$ *e* $a \mid b$.

Tese: $mdc(a,b) = a$.

Mostremos que $a$ satisfaz as duas condições:

i) $a \mid a$ pois $a = a.1$ *e* $a \mid b$ por hipótese.

ii) se $k$ é um número natural tal que $k \mid a$ *e* $k \mid b$, então podemos concluir que $k \mid a$.

Logo, $mdc(a,b) = a$.

■

### 3.4.3 O Algoritmo de Euclides para o cálculo do *mdc*

Como você deve ter percebido pelos exemplos, para encontrar o *mdc* de dois números, devemos conhecer todos os divisores destes dois números. Isto se torna bastante trabalhoso quando estes números têm 5 ou 6 algarismos... O resultado que apresentaremos a seguir nos ensina como encontrar o *mdc* sem que seja necessário conhecer todos os divisores dos números; este resultado dará origem ao Algoritmo de Euclides (ou método das divisões sucessivas), o mais antigo algoritmo que é usado com eficiência desde o século III a. C. Vamos fazer alguns exemplos antes de apresentarmos o algoritmo de maneira formal:

**Exemplo 1.** dados os números 72 e 48, temos que $mdc(72,48)=24$ pois:

divisores de 72: 1, 2, 3, 4, 6, 8, 12, 18, **24**, 36 *e* 72.

divisores de 48: 1, 2, 3, 4, 6, 8, 12, 16, **24** *e* 48.

Pelo Algoritmo da Divisão sabemos que $72=1.48+24$, 1 é o quociente e $24$ é o resto da divisão. Note que $mdc(72,48)=24=mdc(48,24)$ pois $48$ é múltiplo de $24$.

**Exemplo 2.** $mdc(32,12)=4$ pois:

divisores de 32: 1, 2, **4**, 8, 16 *e* 32.

divisores de 12: 1, 2, 3, **4**, 6 *e* 12.

Pelo Algoritmo da Divisão, $32=2.12+8$ e teremos $mdc(32,12)=4=mdc(12,8)$, pois:

divisores de 12: 1, 2, 3, **4**, 6 *e* 12.

divisores de 8: 1, 2, **4** *e* 8.

Assim, os exemplos nos levam à seguinte pergunta: $mdc(a,b)$ será sempre igual ao $mdc(b,r)$, quando $r$ é o resto da divisão euclidiana de $a$ *por* $b$? A resposta está no resultado a seguir:

**Proposição 1.** (Algoritmo de Euclides) Sejam $a$, $b$, $q$ e $r$ números naturais com $b\neq 0$ e $a=b.q+r$, $0\leq r<b$. Então $mdc(a,b)=mdc(b,r)$.

**Demonstração.**

Hipótese: $a,b,q,r \in \mathbb{N}$, $b \neq 0$ *e* $a = b.q + r$, $0 \leq r < b$.

Tese: $mdc(a,b) = mdc(b,r)$.

Seja $d = mdc(a,b)$. Mostremos que $d$ satisfaz as duas condições para ser o $mdc(b,r)$.

i) Como $d = mdc(a,b)$, temos que $d \mid b$. Por hipótese $a = b.q + r$ e como $d \mid a$ e $d \mid b$, temos que $d \mid b.q$ (propriedade D4 de divisibilidade) e consequentemente, $d \mid r$ (propriedade D6 de divisibilidade). Logo, $d \mid b$ *e* $d \mid r$.

ii) Seja $k$ um divisor de $b$ e de $r$. Então $k \mid b.q$ e como $k \mid r$, concluímos que $k \mid b.q + r$ (propriedade D5 de divisibilidade), ou seja, $k \mid a$. Assim, $k$ é um divisor de $a$ e de $b$. Como $d = mdc(a,b)$, $k$ é também um divisor de $d$.

Logo, $mdc(a,b) = d = mdc(b,r)$, quando $r$ é o resto da divisão euclidiana de $a$ por $b$.

■

**Observação 13.** Note que a proposição 1 nos fornece uma "receita" para o cálculo do mdc, uma vez que ela pode ser aplicada repetidas vezes. Note também que, como

$$mdc(a,b) = mdc(b,a),$$

é conveniente tomarmos o maior número como dividendo e o menor como divisor. Veja o exemplo:

**Exemplos**

1) Calcular $mdc(128,82)$

- $128 = 1.82 + 46$; logo, $mdc(128,82) = mdc(82,46)$.
- $82 = 1.46 + 36$; logo, $mdc(128,82) = mdc(82,46) = mdc(46,36)$.
- $46 = 1.36 + 10$; logo, $mdc(128,82) = mdc(82,46) = mdc(46,36) = mdc(36,10)$.
- $36 = 3.10 + 6$; logo, $mdc(128,82) = mdc(82,46) = mdc(46,36) = mdc(36,10) = mdc(10,6)$.

- $10 = 1.6 + 4$ ; logo, $mdc(128,82) = mdc(82,46) = mdc(46,36) =$
  $= mdc(36,10) = mdc(10,6) = mdc(6,4)$ .
- $6 = 1.4 + 2$ ; logo,
  $mdc(128,82) = mdc(82,46) = mdc(46,36) =$
  $= mdc(36,10) = mdc(10,6) = mdc(6,4) = mdc(4,2)$ .
- $a = 2.2 + 0$ ; logo,
  $mdc(128,82) = mdc(82,46) = mdc(46,36) = mdc(36,10) =$
  $= mdc(10,6) = mdc(6,4) = mdc(4,2) = mdc(2,0) = 2$ .

(Note que a última igualdade vale pela propriedade 1).

Assim, $mdc(128,82) = 2$ .

Observe que fazemos várias divisões, sempre utilizando o resto como próximo divisor; encontramos o mdc quando a última divisão for exata, isto é, quando o resto for zero. Podemos reunir estas divisões numa tabela:

| quociente | | 1 | 1 | 1 | 3 | 1 | 1 | 2 |
|---|---|---|---|---|---|---|---|---|
| | **128** | **82** | 46 | 36 | 10 | 6 | 4 | **2** |
| resto | 46 | 36 | 10 | 6 | 4 | **2** | 0 | |

Assim, $mdc(128,82) = 2$ .

2) Calcular $mdc(53,48)$

| quociente | | 1 | 9 | 1 | 1 | 2 |
|---|---|---|---|---|---|---|
| | **53** | **48** | 5 | 3 | 2 | **1** |
| resto | 5 | 3 | 2 | **1** | 0 | |

$mdc(53,48) = 1$ .

**Observação 14.** Note que este processo das divisões sucessivas não corre o risco de se estender indefinidamente, ou seja, é sempre possível encontrar o mdc de dois números. Isto se deve ao fato do processo estar vinculado ao algoritmo da divisão, que limita os restos pelo divisor. Como os divisores são os restos, estes diminuem a cada divisão.

## 3.4.4 Máximo divisor comum de vários números

O *mdc* de dois números consiste no maior divisor (ou fator) destes dois números; isto nos permite calcular o *mdc* de vários números. Por exemplo: qual o maior divisor comum dos números $12, 16, 8$? Observando os divisores vemos que $mdc(12,16,8) = 4$. O processo das divisões sucessivas pode ser aplicado também aqui, fazendo $mdc(12,16,8) = mdc(mdc(16,8),12) = mdc(8,12) = 4$.

Em resumo, calculamos o *mdc* de dois números e, em seguida, calculamos o *mdc* do resultado encontrado e do outro número. Veja mais um exemplo:

**Exemplo**. Calcular $mdc(42,96,58)$. Escolhemos dois destes números para começar, $96$ *e* $42$, por exemplo.

| quociente | | 2 | 3 | 2 |
|---|---|---|---|---|
| | **96** | **42** | 12 | **6** |
| resto | 12 | **6** | 0 | |

Assim, $mdc(96,42) = 6$. Agora calculamos o mdc (6, 58)

| quociente | | 9 | 1 | 2 |
|---|---|---|---|---|
| | **58** | **6** | 4 | **2** |
| resto | 4 | **2** | 0 | |

O $mdc(58,6) = 2$.

Concluímos então que $mdc(42,96,58) = mdc(6,58) = 2$.

Formalmente, escrevemos: "Dados $a$, $b$ e $c$ números naturais, $mdc(a,b,c) = mdc(mdc(a,b),c)$".

## Exercícios propostos

7) Calcule:

a) $mdc(2356,234)$

b) $mdc(123,876,345)$

c) $mdc(491,34)$

8) Determine o maior número natural pelo qual se deve dividir os números 160, 198 e 370 para que os restos sejam respectivamente 7, 11 e 13.

9) Encontre todas as possibilidades para $mdc(m, 5n+6)$, para $n$ um número natural.

## 3.4.5 Máximo divisor comum – resultados importantes

Os resultados e a definição que faremos a seguir serão úteis na resolução de problemas envolvendo $mdc$. Algumas demonstrações mais significativas serão feitas para que você se habitue ao uso das definições e das propriedades de divisibilidade. Outras serão apenas comentadas.

**Números relativamente primos (ou primos entre si)**

Você já observou pelos exemplos que pode ocorrer do $mdc$ de dois (ou mais) números ser igual a 1. Quando isto acontece, dizemos que os números são "relativamente primos".

**Definição.** Sejam $a$ e $b$ números naturais; $a$ e $b$ são relativamente primos se e somente se $mdc(a,b)=1$.

**Exemplos**

1) 21 e 8 são relativamente primos, pois $mdc(21,8)=1$ (faça o cálculo!).

2) Dois números consecutivos são sempre relativamente primos, como 45 e 46, 123 e 124, etc. Vamos provar este fato genericamente:

   Dois números consecutivos podem ser expressos por $n$ e $n+1$. Seja $d=mdc(n,n+1)$.

   Então $d \mid n$ e $d \mid n+1$. Pela propriedade D6 da divisibilidade, temos que $d \mid 1$. Como o único divisor natural de 1 é o próprio 1, concluímos que $d=1$.

**Proposição 2.** Sejam $a, b$ e $k$ números naturais. Se $d=mdc(a,b)$, então $d.k=mdc(a.k,b.k)$.

**Comentário.** Este resultado (que será muito útil para as próximas proposições) nos garante que multiplicando os números $a$ e $b$ por um número $k$, seu $mdc$ também fica multiplicado pelo mesmo $k$; veja alguns exemplos:

a) $mdc(21,8)=1$; $mdc(21.15,8.15)=1.15$, ou seja, $mdc(315,120)=15$.

b) $mdc(12,16)=4$; $mdc(12.10,16.10)=4.10$, ou seja, $mdc(120,160)=40$.

**Proposição 3.** Sejam $a, b$ e $d$ números naturais com $d=mdc(a,b)$. Então os quocientes das divisões de $a$ por $d$ e de $b$ por $d$ são números relativamente primos.

**Demonstração.**

Hipótese: $a,b,d\in\mathbb{N}$, $d=mdc(a,b)$.

Tese: os quocientes das divisões de $a$ por $d$ e de $b$ por $d$ são números relativamente primos.

Como $d=mdc(a,b)$, sabemos que $d\,|\,a$ e $d\,|\,b$. Por definição, existem números naturais $x$ e $y$ tais que $a=d.x$ e $b=d.y$; $x$ e $y$ são os quocientes das divisões de $a$ por $d$ e de $b$ por $d$, respectivamente. Devemos mostrar que $mdc(x,y)=1$.

De fato: $d=mdc(a,b)=mdc(d.x,d.y)$. Pela proposição 2, temos que $d=mdc(d.x,d.y)=d.mdc(x,y)$. Logo, $d.1=d.mdc(x,y)$. Como $d$ é diferente de zero (lembre que $d>0$), podemos cancelá-lo (lembre da lei do cancelamento em $\mathbb{N}$) e teremos $mdc(x,y)=1$, como queríamos demonstrar.

■

## Exercício resolvido

6) Encontre todos os possíveis números naturais cujo produto é $4800$ e cujo $mdc$ é $20$.

**Resolução:** Denotemos os números procurados por $a$ e $b$. O problema nos diz que

i) $mdc(a,b)=20$ e

ii) $a.b=4800$.

De (i), sabemos que $20\,|\,a$ e $20\,|\,b$, ou seja, existem $x$ e $y$ naturais tais que $a=20.x$ e $b=20.y$. Além disso, sabemos que $mdc(x,y)=1$.

Substituindo $a$ e $b$ em (ii), temos:

$$a.b = 4800$$
$$(20.x).(20.y) = 4800$$
$$400.x.y = 4800$$
$$400.x.y = 400.12$$

Pela lei do cancelamento, teremos $x.y = 12$. Se determinarmos $x$ e $y$ podemos determinar $a$ e $b$, uma vez que $a = 20.x$ e $b = 20.y$. Assim, estamos procurando números $x$ e $y$ que satisfaçam $x.y = 12$ e $mdc(x, y) = 1$. Os números naturais que têm produto 12 são: $1.12,\ 2.6,\ 3.4$. Destes, temos dois pares de fatores que são relativamente primos: $1\ e\ 12$ e $3\ e\ 4$. Vamos fazer uma tabela:

| $x$ | $y$ | $a = 20.x$ | $b = 20.y$ | mdc $(a,b)$ |
|---|---|---|---|---|
| 1 | 12 | 20 | 240 | 20 |
| 3 | 4 | 60 | 80 | 20 |

Observe que a última coluna é o "controle": verifique se o $mdc$ é mesmo 20. Caso não seja, você sabe que os números não estão corretos.

Assim, os pares de números satisfazendo as condições do problema são: $20\ e\ 240$ ou $60\ e\ 80$.

**Proposição 4.** Sejam $a, b\ e\ c$ números naturais. Se $a \mid b.c$ e $mdc(a,b) = 1$, então $a \mid c$.

**Demonstração.**

Hipótese: $a, b, c \in \mathbb{N}$, $a \mid b.c$ e $mdc(a,b) = 1$.

Tese: $a \mid c$.

Por hipótese, temos que $mdc(a,b) = 1$; pela proposição 2 concluímos que $mdc(a.c, b.c) = 1.c = c$. Como $a \mid b.c$ por hipótese e $a \mid a.c$ (propriedade de divisibilidade), a segunda parte da definição de mdc nos garante que

$a \mid mdc(a.c, b.c)$. Logo, $a \mid c$.

■

## Exercício resolvido

7) Seja $k$ um número natural. Mostre que se $2|k$ e $3|k$, então $6|k$.

**Resolução.** O exercício nos dá um "critério de divisibilidade" por $6$: se um número é divisível por $2$ e por $3$, ele será divisível por $6$. Vamos provar este fato:

Por hipótese, temos que existem $x$ e $y$ naturais tais que $k = 2.x$ e $k = 3.y$.

Então $2.x = 3.y$. Esta igualdade nos informa que $3|2.x$ e como $mdc(2,3) = 1$, a proposição 4 nos garante que $3|x$, ou seja, existe um $z$ natural tal que $x = 3.z$. Substituindo $x = 3.z$ na igualdade $k = 2.x$ teremos $k = 2.3.z = 6.z$, ou seja, $6|k$.

**Observação 15.** O exercício que acabamos de resolver pode ser generalizado da seguinte maneira:

"Sejam $a, b$ e $k$ números naturais tais que $a|k$, $b|k$ e $mdc(a,b) = 1$. Então $a.b|k$". Isto nos dá critérios de divisibilidade para números que são produtos de números relativamente primos, como por exemplo, $15 = 3.5$, $28 = 4.7$, $42 = 6.7$, etc.

## Exercícios propostos

8) O $mdc$ de dois números naturais é $48$ e o maior deles é $384$. Ache o outro número.

9) Dividindo-se dois números naturais pelo seu $mdc$, a soma dos quocientes obtidos é $8$. Determinar os dois números, sabendo que sua soma é $384$.

10) Quais são as possibilidades para o $mdc$ de dois números naturais dados por $a$ e $2a + 4$?

11) Classifique cada afirmação abaixo em Verdadeira ou Falsa, justificando:

a) O $mdc$ de dois números naturais expressos por $n$ e $2n + 1$ é sempre $1$, para qualquer natural $n$.

b) Considere $a$ e $b$ números naturais. Então $mdc(a, ab + 1) = 2$.

12) O $mdc$ de dois números é 50. Para se chegar a este resultado pelo Algoritmo de Euclides (processo das divisões sucessivas), os quocientes obtidos foram, pela ordem, 1, 2 e 6. Ache os números.

13) Determine todos os possíveis números naturais $n < 20$ tais que $mdc(n, 210) = 1$.

14) Quantos números positivos relativamente primos com 30 e menores do que 30 existem?

## 3.4.6 Máximo Divisor Comum em $\mathbb{Z}$

Como calcular o máximo divisor comum de $-52$ *e* $44$? Vamos fazer pelos divisores inteiros:

- os divisores inteiros de $-52$ são
  $1, 2, \mathbf{4}, 13, 26, 52, -1, -2, -4, -13, -26, -52$ e
- os divisores inteiros de $44$ são
  $1, 2, \mathbf{4}, 11, 22, 44, -1, -2, -4, -11, -22, -44$.

Logo, o $mdc$ de $-52$ *e* $44$ é $4$, assim como o mdc dos números naturais $52$ *e* $44$. O algoritmo de Euclides (das divisões sucessivas) também funciona, desde que utilizemos a divisão euclidiana, ou seja, o algoritmo da divisão no universo dos números inteiros. Lembre que no universo dos números inteiros não fazemos a divisão euclidiana na chave. Vamos verificar:

$$\begin{aligned} -52 &= (-2).44 + 36 \\ 44 &= 1.36 + 8 \\ 36 &= 4.8 + 4 \\ 8 &= 2.4 + 0. \end{aligned}$$

O *mdc* é o divisor da última divisão feita (aquela que tem resto zero), ou seja, $4$. Experimente calcular $mdc(-96, -72)$ pelas divisões sucessivas. Você verá que o resultado coincide com o $mdc(96, 72)$. Isto nos leva a definir o mdc no universo dos números inteiros da seguinte maneira:

**Definição.** Sejam $a$ *e* $b$ números inteiros; um número inteiro $d$ é o máximo divisor comum de $a$ *e* $b$ se e somente se $d$ é o máximo divisor comum do valor absoluto (módulo) de $a$ e de $b$.

**Observação 16.** Lembre que denotamos o valor absoluto ou módulo de $a$ e de $b$ como $|a|$ e $|b|$.

Simbolicamente, para $a$ e $b$ inteiros, podemos escrever: $mdc(a,b) = mdc(|a|,|b|) = d$. Note que isto nos mostra que $d$ é um inteiro positivo.

## 3.4.7 Definições e resultados sobre mdc em $\mathbb{Z}$

**Pergunta:** A definição e os resultados que estudamos no universo dos naturais continuam valendo no universo dos inteiros?

A resposta é sim, de modo geral. Alguns acertos devem ser feitos nos enunciados, para adequar os resultados ao universo dos inteiros. Destacaremos as alterações em negrito.

P1) Se $a$ é um número **inteiro** não nulo, então $mdc(a,0) = |a|$.

P2) Sejam $a$ e $b$ números **inteiros** não nulos simultaneamente. Se $a|b$ então $mdc(a,b) = |a|$.

**Definição.** Sejam $a$ e $b$ números **inteiros**; $a$ e $b$ são relativamente primos se e somente se $mdc(a,b) = 1$.

**Proposição 5.** Sejam $a$, $b$ e $k$ números **inteiros**. Se $d = mdc(a,b)$, então $d.|k| = mdc(a.k, b.k)$.

**Proposição 6.** Sejam $a$, $b$ e $d$ números **inteiros** com $d = mdc(a,b)$. Então os quocientes das divisões **euclidianas** de $a$ por $d$ e de $b$ por $d$ são números relativamente primos.

**Proposição 7.** Sejam $a, b$ e $c$ números **inteiros**. Se $a|b.c$ e $mdc(a,b) = 1$, então $a|c$.

Ao ampliarmos nosso universo para $\mathbb{Z}$, ganhamos um novo resultado muito importante, conhecido como "identidade de Bézout". Este resultado será nosso ponto de partida para a resolução de equações com duas variáveis, conhecidas como equações diofantinas. Vamos fazer alguns exemplos antes de enunciarmos o teorema.

**Exemplos**

1) Se $mdc(-25,15)=5$, podemos encontrar dois números inteiros $s$ e $t$ tais que $5=(-25).s+15.t$; os números $s=-2$ *e* $t=-3$ satisfazem a igualdade pois $(-25).(-2)+15.(-3)=50-45=5$. Note que os números $s$ e $t$ não são únicos! $s=1$ *e* $t=2$ também satisfazem a igualdade pois $(-25).1+15.2=-25+30=5$.

2) $mdc(13,4)=1$; $1=13.s+4.t$. Os números $s=1$ *e* $t=-3$ satisfazem a igualdade pois $13.1+4.(-3)=13-12=1$. Descubra outros números $s$ e $t$ que satisfazem a igualdade.

**Teorema.** (Identidade de Bézout) Sejam $a$, $b$ e $d$ números inteiros e $d=mdc(a,b)$. Então existem $s$ e $t$ inteiros tais que $d=s.a+t.b$.

Nos exemplos que acabamos de fazer, foi fácil encontrar os números $s$ e $t$. Como fazer para encontrar $s$ e $t$ para $mdc(53,48)=1$? A resposta está no algoritmo de Euclides. Utilizando cada uma das divisões sucessivas é possível encontrar $s$ e $t$ por meio de uma série de etapas. Acompanhe o exemplo com atenção:

Para $mdc(53,48)=1$, determinar $s$ e $t$ de modo que $1=53.s+48.t$.

**Passo 1.** Escrever cada uma das divisões sucessivas do algoritmo de Euclides, até que o $mdc$ apareça como resto.

$$53=48.1+5$$
$$48=5.9+3$$
$$5=3.1+2$$
$$3=2.1+1$$

**Passo 2.** Em cada igualdade anterior, isolar o resto como termo da esquerda, sem efetuar os produtos (deixe-os indicados), mantendo o sinal da soma (por exemplo, escreva $(-1).48$ ao invés de $(-48)$.

$$5=53+(-1).48$$
$$3=48+(-9).5$$
$$2=5+(-1).3$$
$$1=3+(-1).2$$

**Passo 3.** Observe a igualdade $1=53.s+48.t$ e compare com a última igualdade do Passo 2: já temos o membro da esquerda. Precisamos

"fazer aparecer" os números 53 e 48. Começando com a igualdade $1 = 3 + (-1).2$ substitua os números 2 e 3 pelas igualdades anteriores do Passo 2. (Observe que 2 e 3 são restos. Muito cuidado com os sinais e **não efetue os produtos**!)

Vejamos:

Temos $1 = 3 + (-1).2$; substituindo 2 e 3 pelo membro direito das igualdades anteriores, ficamos com:

$$1 = [48 + (-9).5] + (-1).[5 + (-1).3].$$

Observe, agora, que o $48$ (um dos números que nos interessa) já apareceu, mas ainda não temos o $53$. Substitua novamente os restos $3$ *e* $5$ mas **não efetue os produtos**! Assim,

$$1 = 48 + (-9).[53 + (-1).48] + (-1).\{[53 + (-1).48] + (-1).[48 + (-9).5]\}.$$

Vamos organizar melhor nossa igualdade, usando a propriedade distributiva, mas deixando que o $48$ e o $53$ fiquem "visíveis":

$$1 = 48 + (-9).53 + (-9).(-1).48 + (-1).[53 + (-1).48 + (-1).48 + (-1).(-9).5].$$

Usando mais uma vez a distributiva (para eliminar os colchetes), temos:

$$1 = 48 + (-9).53 + (-9).(-1).48 + (-1).53 + (-1).(-1).48 + \\ + (-1).(-1).48 + (-1)(-1).(-9).5.$$

Efetuando os produtos, mas deixando $48$ e $53$ "visíveis", faça:

$$1 = 48 + (-9).53 + 9.48 + (-1).53 + 1.48 + 1.48 + (-9).5.$$

Colocando $48$ e $53$ em evidência,

$$1 = 48.(1 + 9 + 1 + 1) + 53[(-9) + (-1)] + (-9).5$$
$$1 = 48.12 + (-10).53 + (-9).5.$$

Observe, agora, que ainda falta mais uma substituição, pois ainda aparece o resto $5$; no lugar do $5$ coloque $5 = 53 + (-1).48$, ou seja:

$$1 = 48.12 + (-10).53 + (-9).[53 + (-1).48].$$

Eliminando os colchetes,

$$1 = 48.12 + (-10).53 + (-9).53 + (-9).(-1).48.$$

Efetuando o produto $(-9).(-1)$ na última parcela, temos:

$$1 = 48.12 + (-10).53 + (-9).53 + 9.48 .$$

Note que, agora, todas as parcelas apresentam o $48$ e o $53$. Colocando-os em evidência, temos:

$$1 = 48.(12 + 9) + 53.[(-10) + (-9)] .$$

Efetuando as adições, temos:

$$1 = 48.21 + 53.(-19) .$$

Portanto,

$$1 = 53.(-19) + 48.21 .$$

Compare a última igualdade com o que estamos procurando: $s$ e $t$ tais que $1 = 53.s + 48.t$. Concluímos, então, que $s = -19$ *e* $t = 21$ satisfazem nossa igualdade inicial.

Observe que este processo deve ser efetuado de forma cuidadosa!

Agora faça você um outro exemplo, usando o procedimento que acabamos de estudar.

## Exercícios propostos

15) Calcule $mdc(54,15)$ e determine pelo algoritmo de Euclides dois números inteiros $s$ e $t$ tais que $mdc(54,15) = 54.s + 15.t$.

16) Considere $a$ e $b$ números inteiros. Mostre que, se existem $s$ e $t$ inteiros tais que $1 = s.a + t.b$, então $mdc(a,b) = 1$.

## 3.4.8 Consequência da Identidade de Bézout: Resolução de Equações Diofantinas

O procedimento de encontrar dois números $s$ *e* $t$ que satisfaçam a identidade de Bézout nos dá a "receita" para resolver certos tipos de equações chamadas Equações **Diofantinas**.

O nome *equação diofantina* é devido a Diofanto, matemático e astrônomo que viveu provavelmente no século III d.C. em Alexandria, no Egito. Em sua obra "Aritmética", Diofanto trata de um conjunto de problemas e seus métodos algébricos de resolução.

De modo geral, uma equação diofantina é uma equação da forma $ax+by=c$, com $a$, $b$ e $c$ números inteiros, $x$ e $y$ as incógnitas; uma solução desta equação é um par de números inteiros $x$ e $y$, denotado por $(x,y)$, que verifica a igualdade. O estudo de equações deste tipo é útil para a resolução de problemas; vamos fazer nosso estudo resolvendo o seguinte problema:

"Quantas mesas para $6$ pessoas e quantas mesas para $4$ pessoas são necessárias para acomodar os $90$ convidados de um jantar, de maneira a usar pelo menos uma mesa de cada tipo?"

Vamos estabelecer os dados do problema; considere:

- $x$: número de mesas para $6$ pessoas
- $y$: número de mesas para $4$ pessoas
- $6x$: quantidade de pessoas que podem ser acomodadas nas mesas para $6$ pessoas
- $4y$: quantidade de pessoas que podem ser acomodadas nas mesas para $4$ pessoas.

Assim, o problema pode ser expresso pela equação $6x+4y=90$. Os termos da equação diofantina são: $a=6$, $b=4$ *e* $c=90$ é chamado o *termo independente* (pois independe das incógnitas). Resolver a equação $6x+4y=90$ é o primeiro passo para resolvermos o problema. Note que, para resolver o problema, os números $x$ e $y$ devem ser positivos pois representam quantidades.

Observe a semelhança da equação $6x+4y=90$ com a identidade de Bézout, $mdc(a,b)=d=\boldsymbol{s}.a+\boldsymbol{t}.b$, na qual $a=6$ e $b=4$ são os números dados, $s$ e $t$ os números procurados (as incógnitas). Sabemos que $mdc(6,4)=2$ e sabemos encontrar $s$ e $t$ tais que $mdc(6,4)=2=6s+4t$. Pergunta: encontrando $s$ e $t$, saberíamos determinar $x$ e $y$ tais que $6x+4y=90$? A resposta é sim. Vamos descrever o procedimento:

**Etapa 1.** Determinação de $s$ *e* $t$:

| quociente | | 1 | 2 |
|---|---|---|---|
| | 6 | 4 | 2 |
| resto | 2 | 0 | |

$$6 = 1.4 + 2$$
$$2 = 6.1 + 4.(-1);\ s = 1\ e\ t = -1$$

Mas a igualdade encontrada não é a nossa equação original $6x + 4y = 90$. Vamos para a

**Etapa 2.** Como $90 = 2.45$, multiplicamos ambos os membros da equação $2 = 6.1 + 4.(-1)$ por $45$:

$$45.2 = 45.[6.1 + 4.(-1)].$$

Não efetue todos os produtos! O $6$ e o $4$ devem ficar visíveis!

$$90 = 6.45 + 4.(-45).$$

Consideremos, nesta equação, os números $x_0 = 45\ e\ y_0 = -45$, com $(x_0, y_0)$ a solução de nossa equação $6x + 4y = 90$ (mas não é a solução do nosso problema!). Note que só foi possível encontrar esta solução pois $90 = 2.45$, ou seja, o termo independente é múltiplo do $mdc$ de $6\ e\ 4$. Isto significa que o processo que acabamos de estudar para encontrar uma solução da equação $6x + 4y = 90$ só funcionou por este motivo: o $mdc$ de $6\ e\ 4$ é divisor de $90$. Este é o primeiro resultado importante na resolução das equações diofantinas:

**Proposição 8.** Sejam *a*, *b* e *c* inteiros. A equação diofantina $ax + by = c$ tem solução se e somente se o máximo divisor comum de *a* e *b* é um divisor de *c*.

**Demonstração.**

1) Hipótese: a equação $ax + by = c$ tem solução.

Tese: $mdc(a,b)$ é um divisor de $c$.

Seja $d = mdc(a,b)$; por hipótese, existe $(x_0, y_0)$ tal que $ax_0 + by_0 = c$. Como $d \mid a$ e $d \mid b$, temos que $d \mid ax_0$ e $d \mid by_0$. Logo, $d \mid ax_0 + by_0$, ou seja, $d \mid c$.

2) Hipótese: $mdc(a,b)$ é um divisor de $c$.

Tese: a equação $ax + by = c$ tem solução.

Devemos encontrar um par de inteiros $(x_0, y_0)$ que satisfaça a igualdade $ax_0 + by_0 = c$.

A "receita" para encontrar este par de números é o processo que estudamos, baseado na identidade de Bézout: se $d = mdc(a,b)$, existem $s$ e $t$ inteiros tais que $d = sa + tb$. Por hipótese, existe $k$ inteiro tal que $c = dk$. Multiplicando ambos os membros da igualdade $d = sa + tb$ por $k$, obtemos $dk = k(sa + tb)$, ou seja, $c = (ks)a + (kt)b$. Assim, encontramos $x_0 = ks$ e $y_0 = kt$ tais que $ax_0 + by_0 = c$. Logo, a equação diofantina tem solução.

■

Mas o fato de encontrarmos uma solução para a equação $6x + 4y = 90$ não resolve o problema proposto, uma vez que a solução encontrada não representa a *quantidade* que necessitamos para dar uma resposta ao problema; como sabemos que outras soluções são possíveis, é razoável perguntarmos: conhecendo uma solução da equação, como posso encontrar uma outra solução que responda a pergunta do problema (no caso, uma solução positiva)? A resposta é sim; para isto vamos enunciar mais um resultado e em seguida utilizá-lo para dar finalmente a resposta ao problema.

**Proposição 9.** Sejam *a*, *b* e *c* números inteiros não nulos e $x_0, y_0$ uma solução da equação $ax + by = c$. Então a equação possui uma infinidade de soluções da forma

$$x = x_0 + b_1 t$$
$$y = y_0 - a_1 t$$

com $d = mdc(a,b)$, $a = d.a_1$, $b = d.b_1$ *e* $t$ qualquer número inteiro.

Além disso, toda solução da equação pode ser expressa desta forma, para cada solução particular $(x_0, y_0)$.

**Comentário.** Este resultado nos garante que toda solução da equação tem esta forma; note que $(x_0, y_0)$ é uma solução particular, $a_1$ *e* $b_1$ são os quocientes da divisão de *a* e *b* pelo *mdc*, respectivamente, e *t* é *qualquer número inteiro*. Assim, para cada valor de *t* teremos uma solução $(x, y)$, dada por

$$\begin{cases} x = x_0 + b_1 t \\ y = y_0 - a_1 t \end{cases}$$ para *t* percorrendo o conjunto $\mathbb{Z}$.

Esta solução $(x, y)$ é chamada a **solução geral** da equação $ax + by = c$.

Conhecendo, agora, a proposição 9, temos condição de procurar uma solução positiva da equação $6x+4y=90$, para resolver o problema. Vamos escrever a solução geral, utilizando a solução particular já encontrada; sabemos que:

$$x_0 = 45\,;\ y_0 = -45\,;\ d = mdc(6,4) = 2\,.$$

Logo, $a = 6 = d.a_1 = 2.3$, ou seja, $a_1 = 3$ e $b = 4 = d.b_1 = 2.2$, ou seja, $b_1 = 2$.

Substituindo $a_1, b_1, x_0$ *e* $y_0$ na solução geral temos:

$$x = 45 + 2.t$$
$$y = -45 - 3.t,\ t \in \mathbb{Z}\,.$$

Esta é a solução geral da equação $6x+4y=90$; isto significa que para *qualquer número inteiro* $t$, o par $(x,y)$ dado por

$$x = 45 + 2t$$
$$y = -45 - 3t$$

é solução da equação $6x+4y=90$.

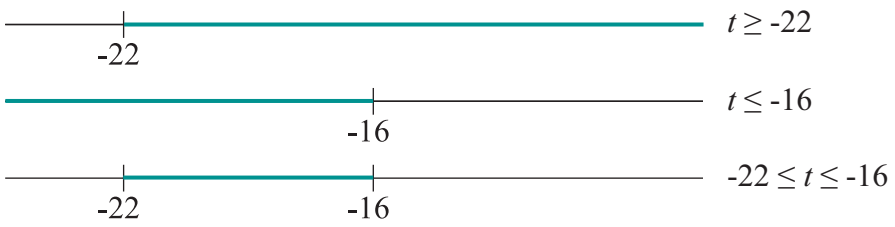
Como toda solução é desta forma, para cada valor de $t$, vamos procurar os valores de $t$ de maneira que $x$ *e* $y$ sejam positivos; em outras palavras, vamos analisar para quais valores de $t$ temos:

$$x = 45 + 2.t > 0 \text{ e também } y = -45 - 3.t > 0\,.$$

i) para que ocorra $x = 45 + 2.t > 0$, devemos ter $45 > -2t$; isto significa que *t* pode assumir todos os valores positivos mas os valores negativos variam de $-1$ *a* $-22$, uma vez que $(-2).(-22) = 44$ e $45 > 44$. Assim, $x = 45 + 2.t > 0$ ocorre para $t \geq -22$.

ii) para que ocorra $y = -45 - 3.t > 0$, devemos ter $-45 > 3t$; isto significa que *t* não pode assumir valores positivos. E a partir de qual valor negativo de *t* ocorre $-45 > 3t$? Para todos os valores negativos estritamente menores do que $-15$, uma vez que $3.(-15) = -45$ e $3.(-16) = -48$ e $-45 > -48$. Assim, $y = -45 - 3.t > 0$ ocorre para $t \leq -16$.

Para que ocorra, *simultaneamente*, $x = 45 + 2.t > 0$ *e* $y = -45 - 3.t > 0$, $t$ deve satisfazer as condições (i) e (ii), ou seja, $t \geq -22$ *e* $t \leq -16$. Veja na reta:




Todos os valores de $t$ entre $-22$ *e* $-16$, inclusive estes, geram soluções positivas da equação $6x + 4y = 90$. Vamos fazer uma tabela para especificar todos eles:

| valores de $t$ | -22 | -21 | -20 | -19 | -18 | -17 | -16 |
|---|---|---|---|---|---|---|---|
| $x$ (mesas p/ 6 pessoas) | 1 | 3 | 5 | 7 | 9 | 11 | 13 |
| $y$ (mesas p/ 4 pessoas) | 21 | 18 | 15 | 12 | 9 | 6 | 3 |

Note a regularidade nos valores de $x$ e $y$: $x$ aumenta de dois em dois e $y$ diminui de três em três. Isto acontece devido às expressões $x = 45 + 2.t$ e $y = -45 - 3.t$.

Temos, então, sete soluções possíveis para o problema; antes de dar a resposta, verifique se realmente estes valores satisfazem a equação $6x + 4y = 90$: é a sua chance de corrigir qualquer erro de conta que possa ter ocorrido. Note que você mesmo pode verificar se acertou ou não o problema!

**Resposta.** Para acomodar os 90 convidados do jantar são necessárias

- 1 mesa para 6 pessoas e 21 mesas para 4 pessoas ou
- 3 mesas para 6 pessoas e 18 mesas para 4 pessoas ou
- 5 mesas para 6 pessoas e 15 mesas para 4 pessoas ou
- 7 mesas para 6 pessoas e 12 mesas para 4 pessoas ou
- 9 mesas para 6 pessoas e 9 mesas para 4 pessoas ou
- 11 mesas para 6 pessoas e 6 mesas para 4 pessoas ou
- 13 mesas para 6 pessoas e 3 mesas para 4 pessoas.

## Exercícios propostos

17) Dar a solução geral das seguintes equações diofantinas:

a) $3x+4y=20$

b) $5x-2y=2$

c) $24x+138y=18$

d) $18x-20y=-8$

e) $-26x+39y=65$

18) Dividir $100$ em duas parcelas positivas de modo que uma seja múltiplo de $7$ e outra seja múltiplo de $11$.

19) Dois tipos de caixa são usados numa fábrica para embalar bolas de futebol: a caixa A para $12$ bolas e a caixa B para $24$ bolas. Quantas caixas de cada tipo são necessárias para embalar $156$ bolas de futebol? Determine todas as possíveis soluções. Se a despesa de envio da caixa A é R$7,00 e a da caixa B é R$10,00, qual a solução mais econômica, usando os dois tipos de caixa?

20) Uma editora usa dois tipos de caixas para transporte de livros: a caixa A para $20$ livros e a caixa B para $100$ livros. Qual a menor quantidade de caixas necessária para embalar $1500$ livros, usando os dois tipos? Quantas caixas de cada tipo?

# 3.5 Mínimo Múltiplo Comum em $\mathbb{N}$ (*mmc*)

Considere o seguinte problema:

Determinar o menor número natural não nulo divisível, simultaneamente, por $12$ e $15$.

**Resolução.** estamos procurando um número $k$ que seja divisível por $12$ e $15$, isto é, que seja múltiplo de $12$ e também múltiplo de $15$. Este número $k$ pode então ser expresso por $k=12.x$ e também por $k=15.y$. Vamos investigar alguns múltiplos de $12$ e de $15$:

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| múltiplos de 12 | 12 | 24 | 36 | 48 | **60** | 72 | 84 |
| múltiplos de 15 | 15 | 30 | 45 | **60** | 75 | 90 | 105 |

Observamos que $60$ é o menor múltiplo natural (e não nulo) de $12$ e de $15$:

$$60 = 12.5 \text{ e } 60 = 15.4.$$

O que acabamos de calcular foi o *mínimo múltiplo comum* (abreviamos por *mmc*) de $12$ e $15$, no conjunto dos números naturais.

**Definição.** Sejam $a$ e $b$ números naturais. Um número natural $m$ é o mínimo múltiplo comum de $a$ e $b$ se, e somente se, são satisfeitas as condições:

i) $m$ é múltiplo de $a$ e $m$ é múltiplo de $b$.

ii) se $c$ é múltiplo de $a$ e $c$ é múltiplo de $b$, então $c$ é múltiplo de $m$.

**Notação.** Quando $m$ é o mínimo múltiplo comum de $a$ e $b$ denotamos $m = mmc(a,b)$.

**Observação 17.** A primeira condição da definição nos informa que para ser o mínimo múltiplo comum de $a$, $b$, $m$ deve ser múltiplo comum; a segunda nos informa que $m$ deve ser o menor deles, ou seja, qualquer outro múltiplo de $a$ e $b$ deve ser também múltiplo de $m$. Note também que, assim como no *mdc*, a ordem em que os números $a$ e $b$ aparecem é irrelevante:

$$mmc(a,b) = mmc(b,a).$$

**Observação 18.** Simbolicamente, a definição pode ser escrita como:

"Sejam $a$ e $b$ números naturais. $m = mmc(a,b)$ se e somente se:

i) $a \mid m$ e $b \mid m$

ii) *Se* $a \mid c$ e $b \mid c$, *então* $m \mid c$."

**Observação 19.** O *mmc* de dois números naturais é único. Este fato é garantido pelo Princípio da Boa Ordenação, estudado no capítulo 2 (lembrando: o Princípio da Boa ordenação garante que existe o menor elemento de todo subconjunto não vazio de números naturais).

**Observação 20.** Note que $mmc(a,0)=0$ pois:

i) $a|0$ *e* $0|0$

ii) seja $c$ um número natural tal que $a|c$ *e* $0|c$. Logo, $0|c$.

(lembre, no entanto, que se $0|c$ devemos ter $c=0$!)

Mas como calcular o $mmc$ de dois números de maneira mais eficiente? Será sempre necessário fazer uma listagem dos múltiplos? A resposta para esta pergunta está na

**Proposição 10.** Sejam $a$ *e* $b$ números naturais não nulos. Então,

$$mdc(a,b).mmc(a,b)=a.b.$$

**Comentário.** O resultado nos diz que, conhecendo o mdc de dois números, podemos calcular o seu $mmc$. Como já sabemos um algoritmo para o cálculo do $mdc$ (o Algoritmo de Euclides), basta calcular o $mdc$ e utilizar a igualdade $mdc(a,b).mmc(a,b)=a.b$ para encontrar o $mmc$.

**Consequências da proposição 10**

**Corolário**
Proposição resultante de uma verdade já demonstrada; conseqüência direta de uma proposição demonstrada.
*Fonte: http://www.priberam.pt/dlpo/dlpo.aspx*

**Corolário 1.** Sejam $a$ *e* $b$ números naturais com $a\neq 0$. Se $a|b$ então $mmc(a,b)=b$.

**Demonstração.**

Hipótese: $a|b$, $a\neq 0$.

Tese. $mmc(a,b)=b$.

Se $a|b$ temos $mdc(a,b)=a$. Pela proposição 5, $a.mmc(a,b)=a.b$.

Como $a\neq 0$, podemos cancelar $a$ em ambos os membros e teremos $mmc(a,b)=b$.

■

**Corolário 2.** Sejam $a, b, d$ *e* $m$ números naturais não nulos, com $d=mdc(a,b)$ e $m=mmc(a,b)$. Se $a=d.x$ e $b=d.y$ com $x$ *e* $y$ relativamente primos então,

$$m=a.y \text{ e } m=b.x.$$

**Demonstração.**

Hipótese: $d = mdc(a,b)$ e $m = mmc(a,b)$, $a = d.x$ e $b = d.y$, com $mdc(x,y) = 1$.

Tese: $m = a.y$ e $m = b.x$.

Por hipótese, $a \mid m$ e $b \mid m$; então existem $c$ e $k$ naturais tais que $m = a.c$ e $m = b.k$.

Mostremos agora que $c = y$ e $k = x$.

Pela proposição 7, temos:

$$d.m = a.b$$

substituindo $m$ por $a.c$ e $b$ por $d.y$, temos

$$d.a.c = a.d.y$$

como $a.d \neq 0$, podemos usar a lei do cancelamento e teremos $c = y$. Use um raciocínio análogo para provar que $k = x$.

■

**Exemplos**

1) Calcular $mmc(65,26)$.

Use o algoritmo de Euclides para calcular $mdc(65,26) = 13$. Então:

$$13.mmc(a,b) = 65.26$$

$$13.mmc(a,b) = 5.13.26$$

Pela lei do cancelamento em $\mathbb{N}$ temos (cancelamos 13 em ambos os membros):

$$mmc(a,b) = 5.26 = 130.$$

2) Calcular $mmc(84,72)$

Já sabemos que $mdc(84,72) = 12$. Então

$$12.mmc(a,b) = 84.72$$
$$12.mmc(a,b) = 84.6.12$$
$$mmc(a,b) = 84.6 = 504$$

## Exercício resolvido

8) Determine todos os possíveis pares de números naturais cujo $mdc$ é $12$ e cujo $mmc$ é $240$.

**Resolução.** Sejam $a$ e $b$ os números procurados; então $mdc(a,b)=12$ e $mmc(a,b)=240$ e teremos:

a) existem $x$ e $y$ naturais tais que $a=12.x$ e $b=12.y$, com $mdc(x,y)=1$.

b) $a|240$ e $b|240$.

c) $12.240=a.b$ (proposição 10)

Substituindo $a$ e $b$ na igualdade em (c), teremos:

$$12.240=12.x.12.y$$
$$12.12.20=12.12.x.y$$

Pela lei do cancelamento em $\mathbb{N}$, $20=x.y$.

Se encontrarmos $x$ e $y$, conheceremos $a$ e $b$; como $mdc(x,y)=1$, estamos procurando dois números relativamente primos cujo produto é $20$. Vamos investigar:

| $x$ | $y$ | $a$ | $b$ |
|---|---|---|---|
| 1 | 20 | 12 | 240 |
| 4 | 5 | 48 | 60 |

**Resposta.** Os pares de números cujo $mdc$ é $12$ e cujo $mmc$ é $240$ são $12$ e $240$ ou $48$ e $60$.

(Verifique se estes valores estão corretos!)

## Exercícios propostos

21) Calcule:

a) $mmc(648,140)$

b) $mmc(132,64)$

22) Mostre que se $a$ e $b$ são números naturais relativamente primos, então $mmc(a,b)=a.b$.

23) Determine todos os números de três algarismos divisíveis por 8, 11 e 12, simultaneamente.

24) Quais são as possibilidades para dois números naturais que têm *mdc* e *mmc* iguais ?

## 3.6 Mínimo Múltiplo Comum em $\mathbb{Z}$

Assim como fizemos para o *mdc*, a definição de *mmc* no conjunto dos números inteiros será dada por:

**Definição.** Sejam $a$ e $b$ números inteiros. Um número inteiro $m$ é o $mmc$ de $a$ e $b$ se e somente se $m$ é o $mmc$ de $|a|$ e $|b|$.

**Observação 21.** Simbolicamente, podemos escrever:
$mmc(a,b) = mmc(|a|,|b|)$. Algumas consequências deste fato são:

i) O $mmc$ de dois inteiros será sempre um número **maior ou igual do que zero**. Se ambos forem não nulos, o $mmc$ será **positivo**.

ii) Como *m* é múltiplo de $|a|$ e $|b|$, *m* é também múltiplo de *a* e *b*.

A proposição 10 e seu corolário 1 continuam valendo em $\mathbb{Z}$, com uma pequena alteração:

**Proposição 11.** Sejam $a$ e $b$ números inteiros não nulos. Então

$$mdc(a,b).mmc(a,b) = |a|.|b|$$

**Corolário.** Sejam $a$ e $b$ inteiros com $a \neq 0$. Se $a|b$ então $mmc(a,b) = |b|$.

**Pergunta:** e quanto ao corolário 2? Vamos observar o que ocorre em um exemplo numérico:

Exemplo: para $a = -26$ e $b = 8$, temos:

$$mdc(-26,8) = mdc(26,8) = 2$$

$$mmc(-26,8) = mmc(26,8) = 104$$

Em relação ao $mdc(-26,8) = 2$, temos que $-26 = 2.(\mathbf{-13})$ e $8 = 2.\mathbf{4}$; logo, $x = -13$ *e* $y = 4$.

Em relação ao $mmc(-26,8)=104$, temos que $104=(-26).(\mathbf{-4})$ e $104=8.\mathbf{13}$. Observe que, neste caso, os valores de $x$ e $y$ relativos ao $mdc$ aparecem "com sinal trocado" no $mmc$. Isto nos leva a crer que o corolário 2 continuará válido em $\mathbb{Z}$, se considerarmos os valores absolutos dos números envolvidos:

Se $|a|=d.|x|$ e $|b|=d.|y|$, então $m=|a|.|y|$ e $m=|b|.|x|$.

## Exercícios propostos

25) Calcule:

a) $mmc(-120,68)$

b) $mmc(-20,-74)$

c) $mdc(-54,125)$

26) Determine o maior número natural pelo qual se devem dividir os números $160$, $198$ *e* $370$ para que os restos sejam respectivamente $7$, $11$ *e* $13$.

27) Determine dois números naturais sabendo que sua soma é $589$ e o quociente entre o $mmc$ e o $mdc$ é $84$.

28) Encontre todos os possíveis pares de números naturais cujo produto é $3600$ e cujo $mmc$ é $1200$.

29) Determine o menor número natural que satisfaça simultaneamente as condições: quando dividido por 2 tem resto 1, quando dividido por 3 tem resto 2, quando dividido por 4 tem resto 3, quando dividido por 5 tem resto 4, quando dividido por 6 tem resto 5, quando dividido por 7 tem resto 6, quando dividido por 8 tem resto 7 e quando dividido por 9 tem resto 8.

30) Determine todos os possíveis números naturais $n$ tais que $mmc(n,54)=54$.

31) O $mmc$ de dois números $a$ *e* $b$ é igual a $1260$ e quando dividimos este $mmc$ pelos números $a$ *e* $b$ o produto dos quocientes obtidos é igual a $90$. Determine todos os números naturais $a$ *e* $b$ satisfazendo esta condição.

32) Determine dois números cuja soma é $120$ e cujo $mmc$ é $144$.

## 3.7 A relação de Congruência módulo *m*

Intuitivamente, uma *relação* é uma comparação entre dois objetos. Os dois objetos estão ou não estão relacionados, de acordo com uma determinada lei. A relação de ordem em $\mathbb{Z}$ é exemplo de como podemos relacionar dois inteiros: podemos dizer que $2$ está relacionado com $5$ pois $2$ *e* $5$ satisfazem a relação $2 \leq 5$. De modo geral utilizamos relações para estudar objetos; estes objetos podem ser números, conjuntos, funções etc.. Neste tópico vamos estudar um tipo especial de relação: a relação de *congruência módulo* $m$, que tem estreita ligação com o Algoritmo da Divisão e, de modo mais geral, com a divisibilidade em $\mathbb{Z}$. Através da congruência podemos resolver problemas interessantes envolvendo números inteiros. Alguns exemplos: em que dia da semana cairá o primeiro dia do século 22? Qual o resto da divisão de $2^{23}$ por $7$?

O conceito de relação é um conceito importante no universo matemático e sua teoria geral será estudada com mais detalhes na disciplina de Introdução ao Cálculo.

**Definição**. Sejam *a*, *b* e *m* números inteiros com $m > 1$. Dizemos que *a é côngruo a* $b$ *módulo* $m$ se e somente se $m$ *é um divisor de* $a - b$.

**Notação.** *"a* é côngruo a *b* módulo *m"* é denotado por $a \equiv b (\text{mód}\, m)$.

**Observação 22.** a definição acima estabelece uma relação para cada valor de $m$; conhecendo o valor de $m$, determinamos a relação. A palavra "módulo" da definição tem o significado de "em relação a": dois inteiros são côngruos *módulo* $m$ é o mesmo que "dois inteiros são côngruos *em relação a* $m$". O termo "módulo" é muito versátil e tem várias conotações em matemática.

**Observação 23.** optamos por estabelecer $m > 1$, uma vez que:

i) para $m = 1$, quaisquer que sejam $a$ *e* $b$ inteiros teremos que 1 é divisor de $a - b$ (lembre: 1 é divisor de todo número inteiro), ou seja, todos os inteiros estão relacionados entre si. Isto torna a relação menos interessante!

ii) para $m = 0$, teremos que cada elemento está relacionado somente com ele próprio, uma vez que o zero não pode fazer

o papel de divisor de números não nulos. Assim, este seria o outro extremo: só teríamos $a \equiv a(\text{mód}\, 0)$. Esta seria a relação de igualdade em $\mathbb{Z}$.

iii) para $m < 0$, lembramos que um número é divisor de outro se e somente se seu oposto é divisor desse número. Assim, se por exemplo $m = -2$, teremos: $a \equiv b(\text{mód}\, -2)$ se e somente se $-2$ é divisor de $a - b$, se e somente se o *oposto de* $-2$ é divisor de $a - b$, o que significa que $2$ é divisor de $a - b$. Desta forma basta considerarmos $m$ positivo e estaremos considerando todas as possíveis relações de congruência módulo $m$.

**Observação 24.** como a relação de congruência está fortemente relacionada com a divisibilidade de inteiros, vamos lembrar a definição de divisor em $\mathbb{Z}$, já estudada anteriormente: "Sejam $x$ *e* $y$ inteiros; dizemos que $x$ é divisor de $y$ se e somente se existe um inteiro $k$ tal que $y = x.k$." (lembre que a notação para "$x$ é divisor de $y$" é $x \mid y$ e lê-se: $x$ divide $y$; note que o traço é vertical, **não é** um traço de fração! Veja os detalhes no início do capítulo 3). Em nossa definição, teremos: $a$ é côngruo a $b$ módulo $m$ se e somente se $m \mid (a - b)$, ou seja, existe um inteiro $k$ tal que $a - b = m.k$.

**Exemplo.** Para $m = 4$, teremos a relação de "congruência módulo $4$ ": $a \equiv b(\text{mód}\, 4)$ se e somente se $4$ é um divisor de $a - b$. Exemplos de alguns inteiros relacionados:

- $45 \equiv 9(\text{mód}\, 4)$ pois 4 é divisor de $45 - 9 = 36$.
- $73 \equiv -7(\text{mód}\, 4)$ pois 4 é divisor de $73 - (-7) = 73 + 7 = 80$.
- $-5 \equiv 3(\text{mód}\, 4)$ pois 4 é divisor de $-5 - 3 = -8$.
- $-25 \equiv -1(\text{mód}\, 4)$ pois 4 é divisor de $-25 - (-1) = -25 + 1 = -24$.

Vamos provar algumas propriedades da relação de congruência módulo $4$; estas propriedades são satisfeitas também por todas as relações de congruência módulo $m$, para qualquer valor de $m > 1$.

i) $a \equiv a(\text{mód}\, 4)$ para todo a inteiro.

**Prova.** Como $4$ é divisor de $a - a = 0$, para todo a inteiro, temos que $a \equiv a(\text{mód}\, 4)$, para todo inteiro $a$. Esta propriedade é chamada *propriedade reflexiva.*

ii) se $a \equiv b(\text{mód } 4)$ então $b \equiv a(\text{mód } 4)$, para todos $a$ e $b$ inteiros.

**Prova.** Hipótese: $a \equiv b(\text{mód } 4)$

Tese. $b \equiv a(\text{mód } 4)$

Por hipótese, temos que $4$ é divisor de $a-b$; então existe um $k$ inteiro tal que

$a-b=4.k$. Logo, $b-a=-(a-b)=4.(-k)$ e $4$ é divisor de $b-a$.

Assim, $b \equiv a(\text{mód } 4)$. Esta propriedade é chamada *propriedade simétrica*.

iii) se $a \equiv b(\text{mód } 4)$ e $b \equiv c(\text{mód } 4)$ então $a \equiv c(\text{mód } 4)$, para quaisquer $a, b$ e $c$ inteiros.

**Prova.** Hipótese: $a \equiv b(\text{mód } 4)$ e $b \equiv c(\text{mód } 4)$

Tese: $a \equiv c(\text{mód } 4)$

Por hipótese, $4$ é divisor de $a-b$ e de $b-c$, ou seja, existem inteiros $s$ e $t$ tais que $a-b=4s$ e $b-c=4t$. Adicionando membro a membro essas igualdades obtemos:

$$(a-b)+(b-c)=4s+4t$$
$$a-b+b-c=4(s+t)$$
$$a-c=4(s-t)$$

o que significa que $4$ é divisor de $a-c$. Logo, $a \equiv c(\text{mód } 4)$.

Esta propriedade é chamada *propriedade transitiva*. Generalizamos estas idéias na proposição que segue.

**Proposição 12.** Seja $m>1$. A relação de congruência módulo $m$ em $\mathbb{Z}$ é reflexiva, simétrica e transitiva, ou seja: para quaisquer inteiros $a, b$ e $c$, temos:

i) $a \equiv a(\text{mód } m)$

ii) se $a \equiv b(\text{mód } m)$ então $b \equiv a(\text{mód } m)$

iii) se $a \equiv b(\text{mód } m)$ e $b \equiv c(\text{mód } m)$ então $a \equiv c(\text{mód } m)$.

**Demonstração.** Faça como exercício, utilizando a idéia da prova anterior.

**Outras propriedades da relação de congruência módulo *m***

Para que a idéia de congruência possa servir de ferramenta para resolver problemas numéricos, precisamos estabelecer algumas propriedades que serão essenciais; faremos alguns exemplos para ilustrar as propriedades e faremos a generalização em seguida. Uma série de exercícios de aplicação destas propriedades será apresentada após a generalização.

**Exemplos**

1) Sabemos que $25 \equiv 4(\text{mód}\,7)$ e $48 \equiv 41(\text{mód}\,7)$, isto é, $7$ é divisor das diferenças $25-4=21$ e $48-41=7$. O que acontece com as somas $25+48$ e $4+41$? Em outras palavras: se "somarmos membro a membro", a congruência se mantém? Vamos investigar:

$$25+48=73$$
$$4+41=45$$
$$73-45=28 \text{ é múltiplo de } 7.$$

Assim, temos que $25+48 \equiv 4+41(\text{mód}\,7)$

E o que acontece se fizermos o produto, membro a membro?

$$25.48=1200$$
$$4.41=164$$
$$1200-164=1036$$
$$1036=7.48 \text{ é múltiplo de } 7.$$

Logo, $(25.48) \equiv (4.41)(\text{mód}\,7)$.

2) Sabemos que $6 \equiv 2(\text{mód}\,4)$ pois $6-2=4$; vamos investigar se as potências de $6$ e $2$ se mantêm côngruas módulo $4$:

$$6^2=36;\ 2^2=4$$
$$36-4=32=4.8 \text{ é múltiplo de } 4.$$

Logo, $6^2 \equiv 2^2(\text{mód}\,4)$.

$$6^3=216;\ 2^3=8$$
$$216-8=208=4.52 \text{ é múltiplo de } 4.$$

Logo, $6^3 \equiv 2^3(\text{mód}\,4)$.

Experimente para as potências $4$, $5$ *e* $6$. Você verá que a congruência se mantém.

Vamos agora generalizar e demonstrar estas propriedades:

PC1) Sejam $a, b, c, d$ *e* $m$ inteiros com $m > 1$. Se $a \equiv b (\text{mód}\, m)$ e $c \equiv d (\text{mód}\, m)$, temos:

1) $(a + c) \equiv (b + d) (\text{mód}\, m)$

2) $(a - c) \equiv (b - d) (\text{mód}\, m)$

3) $a.c \equiv b.d (\text{mód}\, m)$

4) $a^n \equiv b^n (\text{mód}\, m)$, para todo $n \geq 1$.

**Demonstração.**

**(1)** Por hipótese, $a \equiv b (\text{mód}\, m)$ e $c \equiv d (\text{mód}\, m)$, ou seja, $m \mid (a - b)$ e $m \mid (c - d)$. Assim, existem inteiros $x$ e $y$ tais que $a - b = mx$ e $c - d = my$. Adicionando membro a membro as igualdades temos:

$$(a - b) + (c - d) = mx + my$$
$$(a + c) - (b + d) = m(x + y)$$

Logo, $(a + c) \equiv (b + d) (\text{mód}\, m)$.

**(2)** Exercício!

**(3)** Por hipótese, existem inteiros $x$ e $y$ tais que $a - b = mx$ e $c - d = my$; multiplicando a primeira igualdade por $c$ e a segunda por $b$, obtemos $ac - bc = cmx$ e $bc - bd = bmy$. Adicionando membro a membro, temos

$$(ac - bc) + (bc - bd) = cmx - bmy$$

$$ac - bd = m(cx - by)$$

Logo, $ac \equiv b.d (\text{mód}\, m)$.

**(4)** a demonstração será feita no capítulo 5, quando estudarmos o princípio de indução.

PC2) Sejam $a, b$ *e* $m$ inteiros, com $m > 1$. Então $a \equiv b (\text{mód}\, m)$ se e somente se $a$ *e* $b$ têm o mesmo resto na divisão euclidiana por $m$.

**Demonstração.**

($\Rightarrow$) Hipótese: $a \equiv b (\text{mód } m)$

Tese: $a$ e $b$ têm o mesmo resto na divisão euclidiana por $m$, ou seja: existem $x$, $y$ e $r$ inteiros tais que $a = mx + r$ e $b = my + r$, com $0 \leq r < m$.

O Algoritmo da Divisão nos garante que existem $x$, $y$, $r_1$ e $r_2$ tais que: $a = mx + r_1$, $0 \leq r_1 < m$ e $b = my + r_2$, $0 \leq r_2 < m$. (Devemos mostrar agora que $r_1 = r_2$)

Por hipótese, sabemos que $m \mid (a - b)$, ou seja, existe um $k$ inteiro tal que $a - b = km$. Substituindo $a$ e $b$ nessa igualdade, temos:

$$(mx + r_1) - (my + r_2) = km$$
$$mx - my - km = r_2 - r_1$$
$$m(x - y - k) = r_2 - r_1.$$

A última igualdade mostra que $m \mid r_2 - r_1$ e também podemos garantir que $m$ é um divisor de $|r_2 - r_1|$; como $0 \leq r_1 < m$ e $0 \leq r_2 < m$ teremos que a distância entre $r_1$ e $r_2$ é menor do que $m$, ou seja, $|r_2 - r_1| < m$. Ora, se $r_1$ e $r_2$ são diferentes, isto está em contradição com o fato de $m$ ser um divisor $|r_2 - r_1|$ (lembre que se estamos considerando números inteiros positivos, podemos garantir que o divisor é menor que o dividendo, exceto quando o dividendo é zero). Para que esta contradição não ocorra, devemos ter $|r_2 - r_1| = 0$, ou seja, $r_2 = r_1$.

Assim, $a$ e $b$ têm o mesmo resto na divisão por $m$.

($\Leftarrow$) Hipótese: $a$ e $b$ têm o mesmo resto na divisão euclidiana por $m$, ou seja: existem $x$, $y$ e $r$ inteiros tais que $a = mx + r$ e $b = my + r$, com $0 \leq r < m$.

Tese: $a \equiv b (\text{mód } m)$

Para mostrar que $a \equiv b (\text{mód } m)$ devemos observar o que acontece com a diferença $a - b$; usando as igualdades da hipótese, temos:

$$a - b = (mx + r) - (my + r) = mx - my + r - r = mx - my = m(x - y)$$

Logo, $a - b = m(x - y)$ e $m \mid a - b$; por definição, $a \equiv b (\text{mód } m)$.

**Consequência da PC2:** Se $r$ é o resto da divisão de $x$ por $m$, então $x \equiv r$ (mód $m$). Além disso, $r$ é o menor inteiro positivo côngruo a $x$ módulo $m$.

Exemplo: **34** = 4.8 + **2**, logo, **34** ≡**2** (mód 8)

**Exemplo de aplicação das Propriedades 1 e 2:**

Encontre o resto da divisão de $2^{23}$ por $7$, usando as propriedades de congruências.

**Resolução.** seja $r$ o resto procurado; as possibilidades para $r$ são $0, 1, 2, 3, 4, 5$ *ou* $6$. Estamos procurando um $r$ inteiro positivo tal que $2^{23} \equiv r(\text{mód}\,7)$ e $r$ é o menor inteiro positivo nestas condições. Vamos observar os restos na divisão por $7$ das potências de $2$:

$2 \equiv 2(\text{mód}\,7)$ e $2^2 \equiv 4(\text{mód}\,7)$. Usando o teorema 2 (ítem 3), temos que $2^3 \equiv 8(\text{mód}\,7)$; mas $8 \equiv 1(\text{mód}\,7)$ e usando o teorema 1 (iii - transitiva) temos que $2^3 \equiv 1(\text{mód}\,7)$. Usando novamente o teorema 2 (item 4, elevando os dois termos à sétima potência), obtemos $(2^3)^7 \equiv 1^7(\text{mód}\,7)$ que é o mesmo que $2^{21} \equiv 1(\text{mód}\,7)$.

Por que elevamos à sétima potência? Para nos aproximarmos da potência original: $21$ é o múltiplo de $3$ mais "próximo" de $23$ que é menor do que $23$. Mas queremos a potência $23$. Para isso, usamos novamente o teorema 2:

se $2^{21} \equiv 1(\text{mód}\,7)$ e $2^2 \equiv 4(\text{mód}\,7)$ então $2^{21}.2^2 \equiv 1.4(\text{mód}\,7)$.

Com isso, já temos a resposta: $2^{23} \equiv 4(\text{mód}\,7)$ e $4$ é o resto da divisão de $2^{23}$ por $7$. Por que podemos afirmar que $4$ é o resto? Ora, se $2^{23} \equiv 4(\text{mód}\,7)$, temos que $7 \mid (2^{23} - 4)$, ou seja, existe um $k$ inteiro tal que $2^{23} - 4 = 7k$. Assim, $2^{23} = 7k + 4$ e como $0 \leq 4 < 7$, $4$ deverá ser o resto da divisão de $2^{23}$ por $7$.

## Exercícios propostos

33) Encontre o resto da divisão de $5^{42}$ por 8, sem efetuar a conta.

34) Qual o menor inteiro positivo congruente ao produto 11.18.23.22.13.19 módulo $7$?

35) Se $402 \equiv 654(\text{mód}\,m)$, encontre os possíveis valores de $m$.

36) Determine os inteiros $x$, $100 \leq x \leq 200$, tais que $x \equiv -1(\text{mód}\,7)$.

37) Determine o resto da divisão da soma
$$1^5 + 2^5 + 3^5 + \ldots + 100^5 \ \ por\ 4\,.$$

38) Mostre que o resto da divisão de um número inteiro positivo por $10$ é seu algarismo das unidades.

39) Sejam $a$, $b$, $c$, $d$ e $m$ inteiros com $mdc(a,b) = d$ *e* $mmc(a,b) = m$. Prove que:

a) $a \equiv b (\text{mód}\, d)$ b) $a.b \equiv m (\text{mód}\, d)$

40) Mostre que $2^{20} - 1$ é divisível por $41$.

41) Use congruências para verificar que:

a) $89 \mid (2^{44} - 1)$ b) $97 \mid (2^{48} - 1)$

# Resumo

O principal teorema apresentado neste capítulo foi o "Algoritmo da Divisão".

Com este resultado estudamos Divisibilidade, Máximo Divisor Comum, Mínimo Múltiplo Comum e Congruências. Também estudamos as Equações diofantinas cuja resolução é uma aplicação direta do algoritmo de Euclides (cálculo do mdc).

# Bibliografia complementar

DOMINGUES, Hygino H. **Fundamentos de Aritmética**. São Paulo: Atual, 1991.

# Capítulo 4

## Teorema Fundamental da Aritmética

# Capítulo 4

## Teorema Fundamental da Aritmética

*Nosso objetivo neste capítulo é estudar números primos, o Teorema Fundamental da Aritmética e suas aplicações: cálculo do mdc, mmc e do número de divisores. Os resultados aqui desenvolvidos são estudados no universo dos números naturais no Ensino Fundamental e são conhecidos como conseqüências da fatoração.*

## 4.1 Números primos em $\mathbb{N}$ e em $\mathbb{Z}$: diferenças, semelhanças e propriedades

Números primos são conhecidos desde a antiguidade: data de aproximadamente 230 a.C. um dispositivo para identificar números primos, conhecido como o "crivo de Eratóstenes". Nos *Elementos* de Euclides já aparece a definição de número primo, propriedades, e a demonstração da infinitude dos primos. **Pierre de Fermat** (1601-1665) **Leonard Euler** (1707-1783) e muitos matemáticos importantes envolveram-se com este tema, que até hoje atrai mentes brilhantes em todo o mundo. Nos séculos XIX e XX, matemáticos como **George H. Hardy** (1877-1947), **Srinivasa Ramanujan** (1887-1920), **Paul Erdös** (1913-1996), entre outros, também contribuíram para o desenvolvimento da chamada Teoria dos Números, que, é claro, envolve números primos.

**Definição.** (número primo em $\mathbb{N}$) Seja $p$ um número natural; $p$ é primo se e somente se

1) $p \neq 0$ *e* $p \neq 1$ e

2) os únicos divisores de $p$ são $1$ *e* $p$.

**Definição.** (número primo em $\mathbb{Z}$) Seja $p$ um número inteiro; $p$ é primo se e somente se $|p|$ é primo em $\mathbb{N}$.

**Exemplos**:

Em $\mathbb{N}$ os números 13, 23, 37, são primos; provaremos mais adiante que existe uma infinidade de números primos em $\mathbb{N}$. Em $\mathbb{Z}$, serão primos também os opostos dos primos positivos, como –13, –23, –37 etc.

**Considerações sobre as definições**

i) A definição de número primo em $\mathbb{N}$ exclui $0$ *e* $1$ do universo dos primos; os pitagóricos (c.séc. VI a.C.) já excluíam o 1 da condição de primo por acreditar que 1 era o "gerador de todos os números". Não há necessidade de "explicar" porque $0$ *e* $1$ não podem ser primos: eles não o são por definição.

ii) Na definição em $\mathbb{Z}$, note que se $p$ é inteiro e $|\ p\ |$ é primo em $\mathbb{N}$, tem-se:

1) $|p| \neq 0\ e |p| \neq 1$.

2) Os únicos divisores em $\mathbb{N}$ de $|p|$ são $1\ e\ |p|$.

Em (1) temos que $p \neq 0,\ p \neq 1\ e\ p \neq -1$. E que podemos dizer a respeito dos divisores inteiros de $p$? Consideremos $b$ um inteiro divisor de $|p|$; por (2) teremos $|b| = 1$ ou $|b| = |p|$, uma vez que $|b|$ é um número natural.

Usando as propriedades de módulo, concluímos que:

$$b = 1\ ou\ b = -1\ ou\ b = p\ ou\ b = -p\ .$$

Assim, a definição em $\mathbb{Z}$ pode ser enunciada da seguinte forma:

"Seja $p \in \mathbb{Z}$; $p$ é primo se e somente se:

1) $p \neq 0,\ p \neq 1\ e\ p \neq -1$ e

2) os únicos divisores de $p$ são $1, -1, p\ e\ -p$".

iii) Quando um número natural *não* é primo? Como a definição estabelece duas condições, para que um número não seja primo basta que ele não satisfaça uma das condições. Assim, um número natural $n$ não é primo quando $n = 1$, ou $n = 0$, ou $n$ admite pelo menos um divisor diferente de 1 e diferente de $n$.

Quando $n \in \mathbb{N}$, $n > 1$ e $n$ admite pelo menos um divisor diferente de 1 e diferente de $n$, dizemos que $n$ é um número **composto**. Desta forma, um número composto em $\mathbb{N}$ é aquele que pode ser expresso como um produto de números naturais, com fatores diferentes de 1 e do próprio número. O mesmo ocorre em $\mathbb{Z}$: um número inteiro $k$ é composto quando $|k| > 1$ e $k$ pode ser expresso como um produto de inteiros, com fatores diferentes de 1, $-1$, $k$ e $-k$ (veja a definição de divisor no início do capítulo).

Por exemplo, $-99$ é um número composto pois

$$|-99| = 99 > 1 \; e \; -99 = (-3).33 .$$

**Números primos: resultados importantes**

As proposições a seguir são ferramentas essenciais em nosso estudo dos números primos. Elas serão úteis na resolução de exercícios e como argumentos na demonstração de outros resultados.

**Proposição 1.** Dois é um número primo em $\mathbb{N}$.

**Demonstração.**

Seja $b \in \mathbb{N}^*$ um divisor de $2$; então existe $c \in \mathbb{N}$ tal que $2 = b.c$. Pela propriedade D7 (Capítulo 3) temos que $b = |b| \leq |2| = 2$. Se $b \in \mathbb{N}^*$ e $b \leq 2$ devemos ter $b = 1$ *ou* $b = 2$. Assim, os únicos divisores de $2$ em $\mathbb{N}$ são $1$ e o próprio $2$. Logo, $2$ é primo em $\mathbb{N}$.

■

**Observação 1.** Dois é também primo em $\mathbb{Z}$, bem como $-2$. Dois e seu oposto são os únicos primos pares em $\mathbb{Z}$.

**Proposição 2.** Se $n$ é um número inteiro e $|n| > 1$, então n admite um divisor primo.

**Demonstração.**

Sem perda de generalidade, faremos a demonstração em $\mathbb{N}$. Seja $n$ um número natural, $n > 1$, e consideremos o conjunto $S$ dos divisores de $n$ que são maiores do que 1, $S = \{x \in \mathbb{N} / x > 1 \; e \; x | n\}$. Note que $S \neq \varnothing$, uma vez que $n \in S$. Como $S \subset \mathbb{N}$ $e$ $S \neq \varnothing$, o Princípio da Boa Ordenação em $\mathbb{N}$ nos garante que $S$ admite um menor elemento, ou seja, existe $p \in S$ tal que $p \leq x$ para todo $x \in S$. Mostremos

agora que $p$ é um número primo. Para tanto, suponhamos que $p$ não o seja, isto é, suponhamos que existam números naturais $b$ e $c$ tais que $p = b.c$, com $b > 1, c > 1$, $b < p$ e $c < p$. Como $b \mid n$ e $p \mid n$ (pois $p \in S$), temos que $b \mid n$ e portanto $b \in S$. Mas isto significa que encontramos um elemento $b \in S$ que é menor do que o menor elemento de $S$, fato que não pode ocorrer! Logo, nossa suposição de que $p$ não é um número primo revelou-se falsa, ou seja, podemos afirmar que $p$ é primo, como queríamos provar.

■

**Proposição 3.** Sejam $b$ e $p$ números inteiros com $p$ primo. Então:

i) se $p$ não é divisor de $b$, tem-se $mdc(b, p) = 1$,

ii) se $p$ é divisor de $b$, tem-se $mdc(b, p) = |p|$.

**Demonstração.**

Seja $d = mdc(b, p)$. Por definição temos que $d \mid b$ e $d \mid p$. Como $p$ é primo, devemos ter $d = 1$ *ou* $d = |p|$. Se $p$ não é divisor de $b$ então não podemos ter $d = |p|$ e portanto $d = 1$. Se $p$ é divisor de $b$, como $|p| > 1$, teremos $d = |p|$.

■

**Proposição 4.** Sejam $a$, $b$ e $p$ números inteiros; se $p$ é primo e $p$ é divisor do produto $a.b$, então $p$ é divisor de $a$ ou $p$ é divisor de $b$.

**Demonstração.**

Hipótese: $a, b$ e $p$ são números inteiros, $p$ é primo e $p$ é divisor do produto $a.b$.

Tese: $p$ é divisor de $a$ ou $p$ é divisor de $b$.

Por hipótese $p$ é divisor do produto $a.b$, ou seja, existe $x$ inteiro tal que $a.b = p.x$. Suponhamos que $p$ não é divisor de $a$ e provemos que $p$ é divisor de $b$. De fato: como $p$ não é divisor de $a$ e $p$ é primo, a proposição 3 nos garante que $mdc(a, p) = 1$. Mas se $p$ é divisor de $a.b$ e $mdc(a, p) = 1$, $p$ deve ser divisor de $b$ (Proposição 4 do Capítulo 3), como queríamos provar.

■

## 4.2 O Teorema Fundamental da Aritmética

De modo geral, aprendemos a fatorar números na 5ª série; a palavra "fatorar" significa "transformar em produto". Por exemplo, podemos expressar o número $45$ como um produto de $9$ *por* $5$. O produto $9.5$ é uma *fatoração* do número $45$, ou seja, $45 = 9.5$. Ainda na 5ª série, aprendemos que esta transformação em produto pode ser efetuada de modo que todos os fatores sejam números primos. Assim, a fatoração em primos de $45$ seria $45 = 3.3.5$.

**Teorema 1. Teorema Fundamental da Aritmética em $\mathbb{N}$**

Para todo número natural $n > 1$ existem números primos $p_1$, $p_2$, $p_3, \ldots, p_r$ $(r \geq 1)$, de modo que $n = p_1.p_2.p_3.\ldots.p_r$. Além disso, esta decomposição é única a menos da ordem dos fatores.

**Observação 2.** O teorema 1 nos garante que é sempre possível fatorar um número natural estritamente maior do que 1, de modo que todos os fatores sejam números primos. Além disso, o teorema garante que estes primos são únicos, ou seja, não é possível fatorar um mesmo número utilizando dois conjuntos distintos de fatores primos. A demonstração deste teorema decorre da *Proposição 2* e do primeiro princípio de indução, que estudaremos no Capítulo 5.

**Exemplos**

1) Vamos fatorar $342$ em fatores primos. Provavelmente você já conhece o procedimento: procurar os primos que são divisores de $342$; é aconselhável experimentar os primos em sua seqüência: $2, 3, 5, 7, 11, 13, \ldots$ para termos a certeza de não esquecer nenhum (os critérios de divisibilidade são úteis neste momento). Sabemos que $342$ é par; logo, $2$ é um divisor primo: $342 = 2.171$. Mas $171$ é divisível por $3$, $171 = 3.57$. Assim, $342 = 2.171 = 2.3.57$. Vemos que também $57$ é divisível por $3$, isto é, $57 = 3.19$. Logo, $342 = 2.171 = 2.3.57 = 2.3.3.19$.

Observe que todos os fatores deste produto são primos: esta é a decomposição em fatores primos de $342$. De modo geral aprendemos a fazer estas divisões na forma "vertical":

$$\begin{array}{r|l} 342 & 2 \\ 171 & 3 \\ 57 & 3 \\ 19 & 19 \\ 1 & \end{array}$$

À direita do traço vertical ficam os divisores primos; à esquerda, os quocientes das contas de dividir por estes primos. Lemos assim: "$342$ dividido por $2$ dá $171$, que dividido por $3$ resulta $57$, que, por sua vez, quando dividido por $3$ dá $19$, e o único divisor primo de $19$ é o próprio $19$, pois ele é primo". Ao encontrarmos o quociente $1$ a decomposição está completa. Observe que este procedimento "vertical" é apenas uma forma mais simples de escrever as contas que você deverá fazer para encontrar a decomposição, permitindo que você visualize melhor os divisores primos envolvidos. Após fazer a decomposição, podemos agrupar os fatores primos repetidos usando potências; assim, a decomposição de $342$ é: $342 = 2.3.3.19 = 2.3^2.19$. Os primos $2$, $3$ *e* $19$ são os únicos primos envolvidos na fatoração.

2) Fatorar $540$.

Utilizando o procedimento do exemplo 1, fazemos:

$$\begin{array}{r|l} 540 & 2 \\ 270 & 2 \\ 135 & 3 \\ 45 & 3 \\ 15 & 3 \\ 5 & 5 \\ 1 & \end{array}$$

Assim, $540 = 2.2.3.3.3.5 = 2^2.3^3.5$.

**Observação 3.** No processo de fatorar, a ordem em que os divisores primos aparecem não precisa ser necessariamente crescente, uma vez que a multiplicação é comutativa; no exemplo anterior, pode-se começar a fatoração pelo primo $5$, por exemplo:

$$\begin{array}{r|l} 540 & 5 \\ 108 & 2 \\ 54 & 2 \\ 27 & 3 \\ 9 & 3 \\ 3 & 3 \\ 1 & \end{array}$$

A escolha da ordem crescente dos primos é apenas uma sistemática; veremos mais adiante as vantagens desta escolha.

## Exercícios propostos

1) Decomponha em fatores primos os números:
$36938,\ 9999,\ 583,\ 1890,\ 7183,\ 10857,\ 9812,\ 51262,\ 20305$.

2) Qual o menor número natural que possui cinco fatores primos diferentes?

3) Fatore o número $270$ e encontre todos os seus divisores.

**Observação 4.** Note que, no processo de fatorar um número natural, descobrimos todos os seus divisores.

Por exemplo:

$$342 = 2.3^2.19\ .$$

Todo número natural $n$ admite o 1 e o próprio número $n$ como divisores. Estes são chamados *divisores impróprios* de $n$. Os outros possíveis divisores de $n$ são chamados *divisores próprios*.

Pela definição de divisibilidade, são divisores de $342 = 2, 3, 19$, $3^2 = 9$, $2.3 = 6$, $2.3^2 = 18$, $2.19 = 38$, $3.19 = 57$, $3^2.19 = 171$, $2.3.19 = 114$, e os **divisores** $1$ *e* $342$.

***Pergunta.*** *Como fatorar números inteiros negativos?*

Tomemos como exemplo o número $-34$. Utilizando as propriedades dos números inteiros do Capítulo 2, podemos escrever:

$$-34 = (-1).34 = (-1).2.17 = (-2).17 = 2.(-17)\ .$$

Note que os primos envolvidos nas decomposições acima são (lembre que $-1$ não é primo!):

i) em $-34 = (-1).2.17$, os primos $2$ *e* $17$

ii) em $-34 = (-2).17$, os primos $-2$ *e* $17$

iii) em $-34 = 2.(-17)$, os primos $2$ *e* $-17$.

Comparando estas decomposições com a decomposição do número $34$ (oposto de $-34$), que sabemos decompor, vemos que $34 = 2.17$. Assim, *em valor absoluto*, os primos na decomposição de $34$ *e* $-34$ são os mesmos. Isto responde à nossa pergunta de como fatorar inteiros negativos: em valor absoluto, os primos são os mesmos da decomposição de seu oposto positivo. Podemos então enunciar o Teorema Fundamental da Aritmética no universo dos inteiros:

**Teorema 2. Teorema Fundamental da Aritmética em $\mathbb{Z}$**

Seja *b* um número inteiro diferente de 0, 1 e –1. Então, existem números primos positivos $p_1 < p_2 < p_3 < ... < p_r$ e existem números naturais $\alpha_1, \alpha_2, \alpha_3, ..., \alpha_r$, tais que

$$b = E.p_1^{\alpha_1}.p_2^{\alpha_2}...p_r^{\alpha_r}$$

com $E = 1$ se *b* for positivo ou $E = -1$ se *b* for negativo. Além disso, esta decomposição é única.

**Exemplo**: Fatorar $-240$.

Para fatorar $-240$, fazemos $-240 = (-1).240$ e fatoramos $240$ como já vimos. Você pode optar pela fatoração "horizontal":

$$240 = 24.10 = 3.8.2.5 = 3.2.2.2.2.5 = 2^4.3.5.$$

Então $-240 = (-1).2^4.3.5$.

Note que os primos que participam da fatoração de $-240$ são os mesmos que participam da fatoração de $240 = 2, 3$ *e* $5$.

**Observação 5.** A fatoração em $\mathbb{Z}$ também nos permite descobrir todos os divisores de um número inteiro. Por exemplo, $-45 = (-1).5.9 = (-1).3^2.5$; seus divisores são os divisores de $45$ e os opostos destes divisores. Vamos listá-los: $1, 3, 3^2 = 9, 5, 3.5 = 15, 3^2.5 = 45$ e seus opostos $-1, -3, -9, -5, -15, -45$ (um total de 12 divisores, seis positivos e seis negativos).

## Exercício resolvido

1) Determine o menor inteiro positivo $x$, de modo que o produto de $x$ por $6615$ seja um quadrado.

**Resolução.**

Lembre que um quadrado é o resultado do produto de um número por ele mesmo; por exemplo, $25 = 5.5$, $36 = 6.6$, $529 = 23.23$ são quadrados. Também dizemos "$25$ é o quadrado de $5$". No exercício, devemos encontrar um inteiro positivo $x$ de modo que $x.6615$ seja o produto de um número por ele mesmo. Sabemos que tanto $x$ como $6615$ podem ser fatorados, e a fatoração do produto $x.6615$ será o produto das fatorações; isto permitirá descobrir "o que falta" para termos um produto de um número por ele mesmo. Observe:

$$6615 = 3^3.5.7^2 = 3^2.3.5.7^2 = 3^2.7^2.3.5 = (3.7).(3.7).3.5$$

$3^2$ *e* $7^2$ já representam produtos de um número por ele mesmo: $(3.7).(3.7)$. Está "sobrando" um $3.5$, ou melhor, está "faltando" outro $3.5$ para que possamos ter o produto $(3.7).(3.5).(3.7).(3.5)$, que é o quadrado do número $(3.7).(3.5) = 3.3.5.7$. Note também que $3.5 = 15$ é o *menor* número pelo qual devemos multiplicar $6615 = (3.7).(3.7).3.5$ para obter um quadrado. Assim, para $x = 3.5 = 15$, o produto de $x$ por $6615$ é igual ao quadrado de $3.3.5.7 = 315$. Podemos escrever também

$$x.6615 = 15.6615 = 3.5.3^3.5.7^2 = 3^4.5^2.7^2 =$$

$$= (3^2.5.7).(3^2.5.7) = (3^2.5.7)^2.$$

**Observação 6.** O exercício que acabamos de resolver mostra que é possível saber se um número é um quadrado somente observando sua fatoração. Por exemplo: $2^4.3^2.5^6$ é um quadrado, pois podemos escrever $2^4.3^2.5^6 = (2^2.3.5^3)^2$. Assim, podemos dizer que um número é um quadrado quando as *potências* dos primos de sua decomposição são todas *pares*. (Note que estamos usando também uma das propriedades de potência que você estudou no capítulo 2).

## Exercícios propostos

4) Encontre o menor número inteiro positivo pelo qual devemos multiplicar $6776$ de modo que este produto seja a terceira potência de um número.

5) Use a fatoração para determinar todos os divisores inteiros dos números:

   a) 180

   b) 351

   c) 3546

**Teorema 3.** (Euclides) O conjunto dos números primos é infinito.

Antes de demonstrarmos este teorema, precisamos estabelecer a definição de "conjunto infinito". Para tanto, vamos definir quando um conjunto é finito.

**Definição.** Um conjunto $A$ é finito quando podemos encontrar uma correspondência bijetora entre $A$ e o conjunto $S = \{1, 2, 3, 4, \ldots, n\}$. Neste caso podemos expressar o conjunto $A$ como $A = \{a_1, a_2, a_3, \ldots, a_n\}$.

**Observação 7.** A correspondência bijetora que aparece na definição consiste em podermos associar cada elemento de $A$ a um único elemento de $S$, e cada elemento de $S$ a um único elemento de $A$. É a mesma idéia da contagem, quando associamos cada objeto do conjunto que pretendemos contar à lista $1, 2, 3, \ldots, n$. O número $n$ é a quantidade de objetos contados. Assim, um conjunto é finito quando podemos "contá-lo" e ele possui $n$ elementos (sendo $n$ um número natural).

**Definição.** Um conjunto é infinito quando não é finito.

**Observação 8.** Note que, pelas duas definições anteriores, um conjunto possui apenas duas opções: é finito ou infinito. Assim, para provarmos que um conjunto $A$ é infinito, basta provarmos que não é finito, ou seja, que não é possível encontrar uma correspondência bijetora entre $A$ e um conjunto $S = \{1, 2, 3, 4, \ldots, n\}$. Geralmente, para provarmos que um conjunto é infinito, supomos que a correspondência bijetora existe e que sua existência nos leva a uma contradição. Esta é a idéia da demonstração do Teorema 3, apresentada nos *Elementos* de Euclides. Existem outras demonstrações deste teorema, mas a de Euclides continua sendo a mais elegante. Sem perda de generalidade, faremos a demonstração em $\mathbb{N}$.

**Demonstração do Teorema 3.**

Suponhamos que o conjunto $P$ dos números primos em $\mathbb{N}$ é finito. Então podemos expressar $P$ como $P = \{p_1.p_2.p_3.\ldots.p_n\}$ e estes são todos os números primos naturais. Considere agora o número $k = (p_1.p_2.p_3.\ldots.p_n)+1$. Este número é um número natural e, pela Proposição 2, deve ter um divisor primo. Este divisor primo é um dos elementos de $P$: vamos chamá-lo $p_r$. Teremos então que $p_r$ é um divisor de $k = (p_1.p_2.p_3.\ldots.p_n)+1$ e é também um divisor de $p_1, p_2, p_3, \ldots, p_n$, uma vez que é um de seus fatores. Pela propriedade D6 de divisibilidade (se um número é divisor de uma soma e também de uma das parcelas, então é divisor da outra parcela), temos que $p_r$ é um divisor de 1. Como o único divisor natural de 1 é o próprio 1, concluímos que $p_r$ é igual a 1, o que é uma contradição, pois $p_r$ é primo. Esta contradição se originou do fato de supormos $P$ um conjunto finito. Logo, $P$ não é finito, ou seja, é infinito.

■

## Exercícios propostos

6) Prove que o produto de três números consecutivos é divisível por 6.

7) Mostre que o número $a^4+4$ é composto para todo $a$ maior que 1.

8) Se o resto da divisão de um número primo por 3 é 1, mostre que, na divisão deste número por 6, o resto também é 1.

9) Mostre que todo número primo maior que 2 é da forma $4k+1$ *ou* $4k+3$.

10) (Deserto de primos) Considere a seguinte seqüência de números naturais, para $n$ um número natural, $n>1$:

$$a_1 = (n+1)!+2$$
$$a_2 = (n+1)!+3$$
$$a_3 = (n+1)!+4$$
$$\ldots$$
$$a_n = (n+1)!+(n+1)\,.$$

Mostre que $a_1, a_2, a_3, \ldots, a_n$ são números consecutivos e compostos.

# 4.3 Aplicações da Fatoração

O Teorema Fundamental da Aritmética nos garante que podemos decompor um número inteiro em fatores primos (quando este número for diferente de zero, $-1$ *e* $1$) e esta decomposição é única a menos da ordem dos fatores. Expressar números inteiros em produto de primos nos permite obter informações importantes a respeito destes números, como quantos e quais são seus divisores, se o número é um quadrado, um cubo ou outra potência, um cálculo mais eficiente de *mdc e mmc* . Neste tópico estudaremos como obter estas informações por meio da fatoração.

O estudo da divisibilidade já feito no Capítulo 3 será importante; lembramos que quando fatoramos um número, por exemplo, $140$, escrevemos $140 = 2^2.5.7$ e só com isto obtemos as seguintes informações:

1) $140$ é divisível por
$1, 2, 5, 7, 2^2 = 4, 2.5 = 10, 2.7 = 14, 2^2.5 = 20, 2^2.7 = 28, 5.7 = 35$,
$2.5.7 = 70, 2^2.5.7 = 140$.

2) os **únicos** divisores primos de $140$ são $2, 5$ *e* $7$, uma vez que outros primos não aparecem na fatoração.

3) os fatores do produto $2^2.5.7$ são relativamente primos dois a dois, ou seja:

$$mdc(2^2, 5) = mdc(2^2, 7) = mdc(5, 7) = 1 .$$

Faremos nosso estudo das aplicações com exemplos no universo dos números naturais.

**Cálculo do *mdc***

Calcular $mdc(1500, 525)$

Decompomos os números $1500$ *e* $525$ em fatores primos:

$$1500 = 2^2.3.5^3 = 2.2.\mathbf{3}.\mathbf{5}.\mathbf{5}.5$$

$$525 = 3.5^2.7 = \mathbf{3}.\mathbf{5}.\mathbf{5}.7 .$$

Analisamos os fatores primos comuns aos dois números; são eles $3.5.5 = 3.5^2$. Assim, $3.5^2$ é divisor de $1500$ *e* $525$ e é o maior, pois os

outros fatores resultam números relativamente primos: os fatores $2.2.5 = 20$ de $1500$ e o fator $7$ de $525$. Confirme que $mdc(20,7) = 1$. Observe que $3$ *e* $5$ são os fatores primos comuns de $1500$ *e* $525$, mas o $5$ aparece duas vezes na decomposição dos dois números; por isto $3.5^2$ é o maior fator comum (ou divisor comum).

Logo, $mdc(1500,525) = 3.5.5 = 3.5^2 = 75$.

Generalizando este fato, podemos escrever:

"Sejam *a* e *b* números naturais. O *mdc* de *a* e *b* é o produto dos fatores comuns de *a* e de *b*, tomados com os menores expoentes."

**Cálculo do *mmc***

Calcular $mmc(825,315)$

Decompomos os números $825$ *e* $315$ em fatores primos:

$$825 = 3.5^2.11 = 3.5.5.11$$

$$315 = 3^2.5.7 = 3.3.5.7.$$

Como queremos um **múltiplo** comum, os fatores primos que devem aparecer no *mmc* são todos os fatores primos envolvidos na decomposição dos dois números: $3$, $5$, $7$ *e* $11$. Mas, para que o *mmc* seja múltiplo de $825$, o fator $5$ deve aparecer duas vezes; como o *mmc* também deve ser múltiplo de $315$, o fator $3$ deve aparecer duas vezes. Assim, o *mmc* será $3^2.5^2.7.11 = 17325$.

Logo, $mmc(825,315) = 17325$.

Generalizando:

"Sejam *a* e *b* números naturais. O *mmc* de *a* e *b* é o produto de todos os fatores primos que aparecem na decomposição de *a* e de *b*, tomados com os maiores expoentes."

**Número de divisores**

Quantos divisores naturais tem o número $234$?

Decompomos $234$ em fatores primos:

$$234 = 2.3^2.13$$

Os expoentes que aparecem em cada primo da fatoração são 1, 2 e 1. O número de divisores naturais de 234 será dado por: $(1+1).(2+1).(1+1) = 2.3.2 = 12$. Vamos conferir os divisores:

$$1,\ 2,\ 3,\ 13,\ 3^2 = 9,\ 2.3 = 6,\ 2.3^2 = 18,\ 2.13 = 26,$$

$$3.13 = 39,\ 3^2.13 = 117,\ 2.3.13 = 78,\ 2.3^2.13 = 234\,.$$

Note que a *quantidade* de divisores de um número depende da *quantidade* de primos da fatoração e de quantas vezes cada um deles aparece, ou seja, dos *expoentes de cada primo.*

Generalizando:

"Seja $b$ um número natural cuja decomposição em fatores primos é dada por

$$b = p_1^{\alpha_1}.p_2^{\alpha_2}.\ \ldots\ .p_n^{\alpha_n}$$

com $p_1 < p_2 < \ldots < p_n$ primos e naturais.

Então o número de divisores de *b* é:

$$d(b) = (\alpha_1 + 1).(\alpha_2 + 1).\ \ldots\ .(\alpha_n + 1)\,."$$

**Observação importante:** Na decomposição $b = p_1^{\alpha_1}.p_2^{\alpha_2}.\ldots.p_n^{\alpha_n}$ os primos $p_1, p_2, \ldots, p_n$ são todos **diferentes**! O resultado não vale se deixarmos primos iguais como fatores da decomposição.

## Exercícios resolvidos

2) Sejam $m = 2^6.3^3.5^2$, $n = 2^r.3^s.5^t$ e $x = 2^5.5^4$. Escreva as condições que devem satisfazer $r, s\ e\ t$ para que $n$ seja divisor comum de $m\ e\ x$.

**Resolução.** $n = 2^r.3^s.5^t$ deve ser um divisor de $m = 2^6.3^3.5^2$ e de $x = 2^5.5^4$. Para tanto, os primos comuns que aparecem na decomposição de $m\ e\ de\ x$ devem também aparecer na decomposição de $n$; são eles: $2\ e\ 5$. Como $3$ não aparece na decomposição de $x$, já podemos concluir que $s = 0$.

Vamos analisar os expoentes *r* e *t*:

i) expoente $r$

$$m = 2.2.2.2.2.2.3^3.5^2\ \ e\ \ x = 2.2.2.2.2.5^4$$

$2^5$ é a máxima potência de $2$ que divide $m$ e $x$; no entanto, $2^0 = 1,\ 2,\ 2^2,\ 2^3$ e $2^4$ também dividem $m$ e $x$. Assim, devemos ter $0 \le r \le 5$, ou seja, $r$ é igual a $0, 1, 2, 3, 4$ ou $5$.

ii) expoente $t$

$$m = 2^6.3^3.5.5 \text{ e } x = 2^5.5.5.5.5.$$

Analogamente, devemos ter $t$ igual a $0, 1$ ou $2$.

**Resposta.** As condições para os expoentes são: $r$ igual a 0, 1, 2, 3, 4 ou 5; $s = 0$; $t$ igual a $0, 1$ ou $2$.

3) Dados $a = 3^2.19.71^2$, $b = 2.3^5.19.61$ e $c = 2^4.19^2.71$, determine:

a) $mdc(a.b)$

b) $mmc(b,c)$

**Resolução.**

a) $a = 3.3.19.71.71$; $b = 2.3.3.3.3.3.19.61$
$mdc(a,b) = 3.3.19 = 171$

b) $b = 2.3.3.3.3.3.19.61$; $c = 2.2.2.2.19.19.71$
$mmc(b,c) = 2^4.3^5.19^2.61.71$

4) Qual o menor número natural de dois algarismos que admite $8$ divisores?

**Resolução.** Seja $b$ o número procurado, com $d(b) = 8$. Como $d(b)$ é um produto, vamos analisar as possibilidades de produtos que resultam $8$:

i) $d(b) = 8 = 2.4 = (1+1).(3+1)$

Neste caso, teríamos dois primos na decomposição e os expoentes dos primos seriam $1$ e $3$; como queremos o menor número natural de dois algarismos, escolhemos os menores primos, $2$ e $3$, e destinamos o maior expoente para o menor primo. Assim, $b = 2^3.3 = 24$.

ii) $d(b) = 8 = 2.2.2 = (1+1).(1+1).(1+1)$

Já neste caso, teríamos três primos na decomposição, todos com expoente $1$. Os três menores primos são $2, 3$ e $5$. Assim, $b = 2.3.5 = 30$

Como queremos o menor número, concluímos que o número procurado corresponde à possibilidade (i).

**Resposta.** O menor número de dois algarismos que admite $8$ divisores é $24$.

## Exercícios propostos

11) Achar um número $n$ sabendo que satisfaz as condições :

a) $n$ é um cubo

b) $n$ admite 16 divisores

c) na divisão de $n$ por $43$, o quociente é um número primo e o resto é $1$.

12) Considere $a$ *e* $b$ números naturais não relativamente primos, cujo produto é $420$. Determine $mdc(a,b)$.

13) Qual o menor número natural que admite $20$ divisores ?

14) Prove que se um número natural não nulo tem um número ímpar de divisores então ele é um quadrado.

15) Mostre que, se um número natural $a$ é primo, então o número de divisores de $a$ *é* $2$.

16) Determine $r$ *e* $s$ para que $a = 2^3.5^r.7^s$ tenha $84$ divisores.

17) Seja $a$ um número natural que não é divisível por nenhum quadrado diferente de 1 (um número assim é chamado "livre de quadrados"). Se $r$ é o número de fatores primos de $a$ , mostre que $d(a) = 2^r$.

18) Um número $n$ decomposto em fatores primos é da forma $n = 2^x.3^y.5^z$. Ache o número $n$ sabendo-se que se elimina $24$ divisores quando dividimos $n$ por $2$, $18$ divisores quando dividimos $n$ por $3$ *e* $12$ divisores quando dividimos $n$ por $5$.

19) Achar dois números, um com $10$ divisores e outro com $21$ divisores, tal que seu $mdc$ seja $18$.

20) Achar dois números $a$ e $b$ tais que $a^2 + b^2 = 10530$ e $mmc(a,b) = 297$.

## Resumo

Como dito na introdução, estudamos neste capítulo números primos, o Teorema Fundamental da Aritmética e diferentes estratégias de cálculo do *mdc e mmc* usando fatoração. Vimos, também, que a fatoração de um número permite-nos obter informações diversas sobre o número como: quantidade de divisores, se o número é um quadrado, um cubo ou outra potência.

## Bibliografia comentada

DOMINGUES, Hygino H. **Fundamentos de Aritmética**. São Paulo: Atual, 1991.

Este livro, já citado no capítulo anterior, é uma obra que, além de desenvolver o conteúdo, propõe exercícios interessantes. Sugerimos a consulta deste livro ao estudante que busca mais informações sobre o tema.

# Capítulo 5

## Princípio de Indução

# Capítulo 5

## Princípio de Indução

*Neste capítulo, estudaremos o Princípio de Indução, um método de demonstração de teoremas aritméticos, ou, mais rigorosamente, de resultados referentes às propriedades gerais dos números naturais. Muitas vezes, este é o único instrumento adequado para a demonstração de um resultado.*

O método que vamos estudar é conhecido como "Primeiro princípio de indução", uma vez que existe um "Segundo princípio de indução" que não abordaremos aqui. Como você já deve ter percebido, demonstrar afirmações é uma prática em matemática; este particular método de demonstração acompanhará você até o final do curso, aparecendo em, praticamente, todas as disciplinas de conteúdo matemático. Uma característica deste método é que ele se aplica somente a afirmações referentes à sequência de números naturais $0,\ 1,\ 2,\ 3,\ldots$ Veja alguns exemplos de afirmações que podem ser demonstradas usando o Princípio de Indução:

1) $10^n - 1$ é múltiplo de $3$, para todo número natural $n$, $n \geq 0$.
2) $2^n > n^2$, para todo número natural $n \geq 5$.
3) $\cos 2^0\alpha.\cos 2^1\alpha.\cos 2^2\alpha.\cos 2^3\alpha.\ldots.\cos 2^n\alpha = \dfrac{sen(2^{n+1}\alpha)}{2^{n+1}.sen\alpha}$, para todo número natural $n \geq 0$.

Você percebeu algo em comum nestes exemplos?

Todos eles são de afirmações que são verdadeiras *para todo número natural*, a partir de um número natural dado: no exemplo 1, a partir de $0$, no exemplo 2 a partir de $5$ e no exemplo 3 a partir de $0$. Como o conjunto dos números naturais é infinito, não é possível fazer a verificação da veracidade de cada afirmação experimentando *todos* os números naturais! É para afirmações como essas que necessitamos do Princípio de Indução. Em linhas gerais, o Princípio de Indução é um teorema que nos garante que

afirmações deste tipo podem ser provadas para todo número natural a partir de um número dado, sem verifica-los um a um, o que seria impossível. Ao contrário do que parece, é um método *dedutivo* de demonstração. Você conhece o "efeito dominó"? Basta um leve toque no primeiro e todos os outros caem. É com esta idéia que você vai começar a trabalhar agora.

## 5.1 Princípio de Indução

Vocês já viram na disciplina de Problemas - Sistematização e Representação que existem proposições (resultados) gerais e particulares.

Relembremos alguns exemplos de resultados:

1) Resultado geral: Todo número natural terminado em $0$ é divisível por $5$. Resultado particular: $130$ é divisível por $5$.
2) Resultado geral: Todo ser humano é mortal.
   Resultado particular: você é mortal.

No primeiro exemplo, do fato de "Todo número natural terminado em $0$ é divisível por $5$" ser verdadeira, deduzimos que "$130$ é divisível por $5$", também é verdadeiro, pois $130$ termina em $0$ (zero).

"Todo número natural terminado em $0$ é divisível por $5$"

$130$ é um número natural terminado em $0$.

Logo: $130$ é divisível por $5$.

O raciocínio de passar do geral ao particular é chamado "dedução". Se a afirmação é verdadeira no caso geral, também será em casos particulares.

Observemos os seguintes exemplos:

1) É possível estabelecer um resultado geral para a soma dos '$n$' primeiros números ímpares?

$$1+3+5+\ldots+(2n-1)=?$$

Vamos analisar casos particulares:

$$\begin{aligned} n=1, &\quad 1=1=1^2 \\ n=2, &\quad 1+3=4=2^2 \\ n=3, &\quad 1+3+5=9=3^2 \\ n=4, &\quad 1+3+5+7=16=4^2 \\ n=5, &\quad 1+3+5+7+9=25=5^2. \end{aligned}$$

É razoável pensar que, ao somar $n$ ímpares o valor da soma será $n^2$, com '$n$' sendo o número de parcelas somadas.

No entanto, esta é apenas uma conjectura. Existe um abismo entre "provavelmente verdadeiro" e "absolutamente verdadeiro".

É necessário um argumento lógico que nos garanta a validade da afirmação:

$1+3+5+\ldots+(2n-1)=n^2$, para todo valor de $n$, $n \geq 1$.

2) Observemos agora a afirmação:

$x=n^2+n+41$ é um número primo $\forall n \geq 0$.

Casos particulares:

$$\begin{aligned} n=0, &\Rightarrow x=41 \\ n=1, &\Rightarrow x=43 \\ n=2, &\Rightarrow x=47 \\ n=3, &\Rightarrow x=53 \\ n=4, &\Rightarrow x=61 \\ n=5, &\Rightarrow x=71 \\ n=6, &\Rightarrow x=83 \\ n=7, &\Rightarrow x=97 \\ n=8, &\Rightarrow x=113 \\ n=9, &\Rightarrow x=131 \\ &\ldots \end{aligned}$$

Mas, para $n=40$, teremos

$$40^2+40+41=40(40+1)+41=40.41+41=$$

$=41(40+1)=41.41$ é um número composto!

Apesar de "parecer" verdadeira (e é para os primeiros $39$ valores de $n$), a afirmação não se verifica para todo $n \geq 0$.

3) Analisemos as afirmações:

$n^3 - n$ é divisível por $3$,

$n^5 - n$ é divisível por $5$

$n^7 - n$ é divisível por $7$

…

Parece razoável que $n^k - n$ é divisível por $k$, $\forall k$ ímpar, $\forall n \geq 1$, mas $2^9 - 2 = 510$ não é divisível por $9$!

**Conclusão:** Uma proposição pode ser válida em uma série de casos particulares e não ser válida em geral.

**Questão:** Como garantir que uma proposição geral é verdadeira para todo número natural '*n*', se não podemos experimentar todos os valores possíveis de '*n*'?

**Resposta:** Às vezes (mas nem sempre) podemos garantir a validade aplicando um argumento especial, chamado "Princípio de Indução". Vamos aplicar este argumento em nosso primeiro exemplo. Leia com atenção.

**Exemplos:**

1) Prove que $1+3+5+\ldots+(2n-1) = n^2$, para todo $n \geq 1$.

1°) Verificamos se a afirmação é verdadeira para o primeiro número natural envolvido, no caso $n = 1$;

$$1 = 1^2 \text{ é verdadeiro.}$$

Note que $n = 1$ significa que estamos considerando a "soma" de uma parcela.

2°) Sendo $k$ um valor para o qual a afirmação é verdadeira, $k$ fixo, $k \geq 1$, verificamos se ela continua válida para $k+1$, número natural que segue imediatamente.

Suponhamos que:

$$1+3+5+\ldots+(2k-1)+(2k+1)=(k+1)^2,$$

(ou seja, a igualdade é verdadeira para a soma de $k$ parcelas de números ímpares).

Acrescentamos mais um ímpar à soma, ficando com $k+1$ parcelas ímpares. Nosso objetivo agora é provar a igualdade $1+3+5+\ldots+(2k-1)+(2k+1)=k^2$, isto é, que a nossa afirmação original é verdadeira para $k+1$ parcelas. Note que o número ímpar que segue $2k-1$ é $2k+1$.

$$\underbrace{1+3+\ldots+(2k-1)}_{\text{esta parcela é igual a } k^2}+(2k+1)=k^2+2k+1=(k+1)^2.$$

Note que a última igualdade se deve ao fato de $(k+1)^2=k^2+2k+1$ (Trinômio Quadrado Perfeito).

Assim, podemos garantir que a afirmação vale para $n=1$, $n=2$, $n=3,\ldots$ etc, isto é, a afirmação é verdadeira para todo $n\geq 1$.

**Observação.** Neste exemplo, fizemos nosso raciocínio de indução sobre a quantidade de parcelas (de números ímpares) que estavam sendo somados.

Em resumo, para provar que a soma dos primeiros '$n$' números ímpares é igual a $n^2$, para todo $n\geq 1$, fizemos o seguinte:

1°) Verificamos que a igualdade era verdadeira para uma parcela ($n=1$).

2°) Supomos a igualdade verdadeira para $k$ parcelas, chamamos esta suposição de Hipótese de Indução. Este fato nos levou a concluir que a igualdade também era verdadeira para $k+1$ parcelas, ou seja, que a soma dos $k+1$ primeiros números ímpares era igual a $(k+1)^2$.

Se provarmos a igualdade para o primeiro valor de '$n$' ($n=1$) provamos que, valendo para um valor $k$ fixo também vale para $k+1$, podemos concluir que a igualdade é verdadeira para $1+1=2$, $2+1=3$, $3+1=4$ etc; isto nos garante que a igualdade $n$ é verdadeira para todo valor de $n\geq 1$.

2) $10^n - 1$ é múltiplo de $3$ para todo $n \geq 1$.

Faremos a indução sobre '$n$', a potência de $10$.

1°) para $n = 1$, $10^1 - 1 = 9 = 3.3$

Logo, $10^1 - 1$ é múltiplo de $3$.

2°) Hipótese de Indução: Consideremos válido para $k$ fixo, $k \geq 1$: $10^k - 1$ é múltiplo de $3$, ou seja, $10^k - 1 = 3y$, para algum $y$ natural.

Nosso objetivo é mostrar que $10^{k+1} - 1$ também é múltiplo de $3$, ou seja, devemos mostrar a existência de um número natural $x$ tal que $10^{k+1} - 1 = 3x$. Para provar esta igualdade, vamos desenvolver o membro da esquerda e usar nossa Hipótese.

$$10^{k+1} - 1 = 10^k.10 - 1 =$$
$$= 10^k.(9+1) - 1 = 9.10^k + \underbrace{10^k - 1}_{HI} =$$
$$= 9.10^k + 3y = 3(\underbrace{3.10^k + y}_{x}) = 3x.$$

Logo, $10^n - 1$ é múltiplo de $3$.

De 1°) e 2°) concluímos que $10^n - 1$ é múltiplo de $3$ para todo $n \geq 1$.

3) $3^n - 1$ é múltiplo de $2$, para todo $n \geq 1$.

Para $n = 1$ temos que: $3^1 - 1 = 2$; $2$ é múltiplo de $2$. Logo, vale para $n = 1$.

Hipótese de indução: $k$ fixo, $k \geq 1$; $3^k - 1$ é múltiplo de $2$, ou seja: $3^k - 1 = 2y$, para algum $y \in \mathbb{N}$.

Nosso objetivo é mostrar que $3^{k+1} - 1 = 3x$ para algum $x$ natural. Análogo ao exemplo anterior, fazemos:

$$3^{k+1} - 1 = 3^k.3 - 1 = 3^k.(2+1) - 1$$
$$= 2.3^k + \underbrace{3^k - 1}_{HI} = 2.3^k + 2y =$$
$$= 2(3^k + y) = 2x.$$

Logo: $3^n - 1$ é múltiplo de $2$, $\forall n \geq 1$.

Vamos enunciar o Princípio de Indução:

**Princípio de Indução**

Seja a um número inteiro.

Uma proposição é verdadeira para todo inteiro n ≥ a se são verificadas as condições:

1) A proposição é verdadeira para a (o primeiro inteiro envolvido).
2) Admitindo a proposição válida para um número $k \geq a$, provamos sua validade para $k + 1$ (o número consecutivo).

**Mais exemplos**

4) $1+2+3+\ldots+n=\frac{n(n+1)}{2}$, $\forall n \geq 1$ ($n$ é a quantidade de naturais consecutivos somados).

1°) $n=1$, $\frac{1(1+1)}{2}=\frac{2}{2}=1$. OK.

2°) Hipótese de indução: para $k$ fixo, $k \geq 1$,

$$1+2+3+\ldots+k=\frac{k(k+1)}{2}.$$

Nosso objetivo, agora, é provar que a igualdade é verdadeira se acrescentarmos mais uma parcela. Note que estamos fazendo a indução sobre a quantidade de parcelas somadas. Assim, o que queremos provar é a igualdade,

$$1+2+\ldots+k+(k+1)=\frac{(k+1)(k+2)}{2}.$$

Vamos desenvolver o membro da esquerda e usar a hipótese de indução.

$$\underbrace{1+2+3+\ldots+k}_{HI}+(k+1)=\frac{k(k+1)}{2}+(k+1)=$$

$$=\frac{k}{2}(k+1)+(k+1)=(k+1)(\frac{k}{2}+1)=$$

$$=(k+1)(\frac{k+2}{2})=\frac{(k+1)(k+2)}{2}.$$

Assim, a igualdade é verdadeira para $k+1$.

Logo, $1+2+...+n=\dfrac{n(n+1)}{2}$ é verdadeira para todo $n\geq 1$.

5) $7$ é divisor de $2^{3n}-1, \forall n\geq 0$

1°) Para $n=0$, $2^{3.0}-1=1-1=7.0=0$. Logo vale para $n=0$.

2°) Hipótese de indução: para $k$ fixo, $k\geq 0$, $7$ é divisor de $2^{3k}-1$, ou seja, $2^{3k}-1=7y$, para algum $y\in\mathbb{N}$.

Nosso objetivo é mostrar que $2^{3(k+1)}-1=7x$ para algum $x\in\mathbb{N}$.

$$2^{3(k+1)}-1=2^{3k+3}-1=2^{3k}.2^3-1=$$
$$=2^{3k}.8-1=2^{3k}(7+1)-1=7.2^{3k}+\underbrace{2^{3k}-1}_{HI}=$$
$$=7.2^{3k}+7y=7\underbrace{(2^{3k}+y)}_{x}=7x\ .$$

Logo , $7$ é divisor de $2^{3n}-1, \forall n\geq 0$.

6) $1.2+2.3+3.4+...+n(n+1)=\dfrac{1}{3}(n+1)(n+2)n$, $\forall n\geq 1$

A indução aqui será feita sobre o número de parcelas somadas.

1°) Para $n=1$, $\dfrac{1}{3}(1+1)(1+2).1=\dfrac{1}{3}(2)(3).1=\dfrac{6}{3}.1=2.1$. Logo vale para $n=1$ (uma parcela).

2°) Hipótese de indução: para $k$ fixo, $k\geq 1$,

$$1.2+2.3+3.4+...+k(k+1)=\frac{1}{3}(k+1)(k+2)k\ .$$

Nosso objetivo é provar a igualdade

$$1.2+...+k(k+1)+(k+1)(k+2)=\frac{(k+1)(k+2)(k+3)}{3}\ .$$

Vamos desenvolver o membro da esquerda e usar a Hipótese; note que a parcela acrescentada é o produto $(k+1)(k+2)$.

$$1.2+2.3+\ldots+k(k+1)+(k+1)(k+2)=$$
$$=\frac{1}{3}(k+1)(k+2)k+(k+1)(k+2)=$$
$$=(k+1)(k+2)\left[\frac{1}{3}k+1\right]=(k+1)(k+2)\left[\frac{k+3}{3}\right]=$$
$$=\frac{(k+1)(k+2)(k+3)}{3}$$

Logo, $1.2+2.3+3.4+\ldots+n(n+1)=\frac{1}{3}(n+1)(n+2)n$, $\forall n\geq 1$.

7) Demonstração de Propriedades das Potências

**Propriedade.** Seja $x\in\mathbb{N}^*$, $n,m\in\mathbb{N}$. Então:

a) $x^n.x^m=x^{n+m}$

b) $(x^n)^m=x^{n.m}$

Antes de provar estas propriedades, vejamos primeiramente a seguinte definição de potência de um número inteiro:

**Definição.** Para '$x$' um número inteiro e '$n$' um número natural, definimos:

$$\begin{cases} x^0=1 \ \ para\ n=0 \\ x^1=x \ \ para\ n=1 \\ x^{n+1}=x^n.x \ \ para\ n>1\ . \end{cases}$$

**Exemplo.** $5^4=5^3.5=(5^2.5).5=[(5.5).5].5=25.5.5=625$

Note que esta é uma definição "por recorrência" como a definição de adição vista no capítulo 2.

Vejamos, agora, as demonstrações:

a) Consideramos '$n$' fixo e fazemos a indução sobre '$m$'.

1°) Para $m=0$, $x^n.x^0=x^n.1=x^n=x^{n+0}$. Logo, a afirmação é verdadeira para $m=0$.

2°) Hipótese de indução: para $k$ fixo, $k\geq 0: x^n.x^k=x^{n+k}$

Nosso objetivo é mostrar que a afirmação é verdadeira para $k+1$, ou seja, $x^n.x^{k+1} = x^{n+(k+1)}$. Para provar esta igualdade, vamos desenvolver o membro da esquerda e usar a Hipótese de indução.

$$x^n.x^{k+1} = x^n.x^k.x \overset{HI}{=} (x^n.x^k).x =$$
$$= x^{n+k}.x \overset{Def.}{=} x^{(n+k)+1} = x^{n+(k+1)}.$$

Logo, a afirmação é verdadeira para todo $n \geq 0$.

b) Consideramos '$n$' fixo e fazemos a indução sobre '$m$':

1°) Para $m = 0$, $(x^n)^0 = 1$ e $x^{n.0} = x^0 = 1$. Logo, $(x^n)^0 = x^{n.0} = 1$.

2°) Hipótese de Indução: para $k$ fixo, $k \geq 0$, $(x^n)^k = x^{n.k}$.

Nosso objetivo é mostrar que a afirmação é verdadeira para $k+1$, ou seja, $(x^n)^{k+1} = x^{n(k+1)}$. Para provar esta igualdade, vamos desenvolver o membro da esquerda e usar a hipótese de indução.

$$(x^n)^{k+1} = (x^n)^k.(x^n)^1 \overset{HI}{=} x^{n.k}.x^n \overset{a)}{=}$$
$$= x^{nk+n} = x^{n.(k+1)}.$$

Logo, a afirmação é verdadeira para todo $m \geq 0$.

8) Demonstração da propriedade da congruência

Sejam $a$, $b$ e $m$ inteiros, $m > 1$.

Se $a \equiv b (\text{mód}\, m)$ então, $a^n \equiv b^n (\text{mód}\, m)$, para todo $n \geq 1$.

**Demonstração:**

1°) Para $n = 1$, a afirmação é verdadeira por hipótese.

2°) Hipótese de indução: Suponhamos a afirmação verdadeira para $k$ fixo, $k \geq 1$: $a^k \equiv b^k (\text{mód}\, m)$.

Nosso objetivo é mostrar que $a^{k+1} \equiv b^{k+1} (\text{mód}\, m)$.

Como $a \equiv b (\text{mód}\, m)$ por hipótese e $a^k \equiv b^k (\text{mód}\, m)$ pela Hipótese de Indução, usando o item anterior temos:

$$a.a^k \equiv b.b^k (\text{mód}\, m), \ ou\ seja,$$
$$a^{k+1} \equiv b^{k+1} (\text{mód}\, m)$$

Logo, a afirmação é verdadeira para todo $n \geq 1$.

## Exercícios propostos

1) Prove que: $n^3 - n$ é divisível por $6$, $\forall n \geq 1$.

2) Prove que: 11 é divisor de $2^{2n-1}.3^{n+2} + 1, \forall n \geq 1$.

3) Prove que: $1 + 2 + 2^2 + 2^3 + ... + 2^{n-1} = 2^n - 1$, $\forall n \geq 1$.

4) Prove que: $1^2 + 2^2 + 3^2 + ... + n^2 = \frac{n(2n+1)(n+1)}{6}$, $\forall n \geq 1$.

5) Prove que: $2^n > n^2$, $\forall n \geq 5$.

# Resumo

Estudamos, neste capítulo, um método de demonstração, chamado: "Primeiro princípio de indução" que consiste do seguinte:

"Seja $a$ um número inteiro.

Uma proposição é verdadeira para todo inteiro $n \geq a$ se são verificadas as condições:

1) A proposição é verdadeira para $a$ (o primeiro inteiro envolvido).

2) Admitindo a proposição válida para um número $k \geq a$, provamos sua validade para $k+1$ (o número consecutivo)."

Você deve ter percebido a tipologia das afirmações, para as quais, o princípio da indução se mostra como uma forma adequada e eficiente para fazer demonstrações.

# Bibliografia comentada

SOMINSKI, I. S. **Método de indução matemática.** São Paulo: Atual, 1996.

Neste livro você encontra vários exemplos de resultados demonstrados pelo método de indução estudado aqui.

# Capítulo 6

## Números racionais

# Capítulo 6

## Números racionais

*Neste texto, faremos um estudo do conjunto dos números racionais a partir da idéia de fração. As operações e a relação de ordem serão trabalhadas nas duas representações: decimal e fracionária. Também apresentaremos as propriedades relativas às operações.*

## 6.1 Introdução

Os números racionais aparecem pela primeira vez nas séries iniciais do Ensino Fundamental, com a idéia de "fração"; na quinta e na sexta séries do Ensino Fundamental o assunto é retomado sob o ponto de vista de um conjunto numérico com operações próprias e novos algoritmos. O que era o "pedaço de um todo" passa a ser tratado como número. É um assunto que requer uma abordagem cuidadosa para que o estudante possa fazer essa transição de modo natural. Muito importante também neste contexto são as diferentes representações de um número racional.

Historicamente, os números racionais já aparecem nos mais antigos registros. Em 2000 a.C. os babilônios já usavam frações, essencialmente como as usamos hoje; aos egípcios se credita o primeiro tratamento sistemático das frações (papiro de Rhind, cerca de 1700 a.C.) referente a frações unitárias (frações com numerador igual a 1). Os gregos possuíam notações especiais para as frações (escreviam somente o denominador das frações unitárias) e os romanos usavam em geral frações de denominador 12. Cálculos com frações constituíam a parte principal da instrução matemática nas escolas romanas. O modo atual de representar as frações provavelmente originou-se na civilização indiana.

No século VI, o denominador era escrito acima do numerador, sem o traço; por volta do ano 1000 de nossa era, os árabes introduziram o traço separando numerador de denominador. Em

1585, **Simon Stevin** apresentou ao ocidente a notação decimal como a conhecemos hoje, que se originou da representação de uma fração como soma de frações cujos denominadores são potências de 10 e cujos numeradores são os algarismos. Esta notação universalizou-se somente no século XVIII, apesar das vantagens que tem sobre a notação em forma de fração. Até hoje existem pequenas diferenças relativas à notação decimal; por exemplo, os americanos usam o ponto e nós usamos a vírgula para separar a parte inteira da parte fracionária: eles escrevem 2.1 e nós escrevemos 2,1 para representar dois inteiros e um décimo.

Assim como nos outros textos dessa disciplina, aconselhamos o leitor a estudá-lo com lápis e papel na mão; uma calculadora simples também pode ser útil.

## 6.2 A idéia da construção do conjunto dos números racionais

A idéia da construção do conjunto dos números racionais é semelhante àquela apresentada na construção do conjunto dos números inteiros: utilizar o que "falta" em $\mathbb{Z}$ para gerar novos números, formando um conjunto mais amplo, no qual o "defeito" de $\mathbb{Z}$ não aparece. Mas qual é o "defeito"? O que "falta" em $\mathbb{Z}$? Assim como em $\mathbb{N}$ nem sempre podemos subtrair, em $\mathbb{Z}$ nem sempre podemos dividir. Ou seja: as equações da forma $a+x=b$ com $a$ e $b$ naturais nem sempre têm solução em $\mathbb{N}$ (só têm solução em $\mathbb{N}$ quando $b \geq a$) e as equações da forma $bx=a$ com $a$ e $b$ inteiros nem sempre têm solução em $\mathbb{Z}$ (têm solução em $\mathbb{Z}$ quando $b \mid a$). Analogamente ao processo do capítulo 2, "acrescentamos" ao conjunto $\mathbb{Z}$ todas as soluções das equações da forma $bx=a$ com $a$ e $b$ inteiros. Vamos observar as equações desta forma:

| | | | | | | |
|---|---|---|---|---|---|---|
| $1x=0$ | $2x=0$ | $3x=0$ | $\cdots$ | $(-1)x=0$ | $(-2)x=0$ | $\cdots$ |
| $1x=1$ | $2x=1$ | $3x=1$ | $\cdots$ | $(-1)x=1$ | $(-2)x=1$ | $\cdots$ |
| $1x=2$ | $2x=2$ | $3x=2$ | $\cdots$ | $(-1)x=2$ | $(-2)x=2$ | $\cdots$ |
| $1x=3$ | $2x=3$ | $3x=3$ | $\cdots$ | $(-1)x=3$ | $(-2)x=3$ | $\cdots$ |
| $\cdots$ | $\cdots$ | $\cdots$ | $\cdots$ | $\cdots$ | $\cdots$ | $\cdots$ |
| $1x=-1$ | $2x=-1$ | $3x=-1$ | $\cdots$ | $(-1)x=-1$ | $(-2)x=-1$ | $\cdots$ |
| $1x=-2$ | $2x=-2$ | $3x=-2$ | $\cdots$ | $(-1)x=-2$ | $(-2)x=-2$ | $\cdots$ |
| $1x=-3$ | $2x=-3$ | $3x=-3$ | $\cdots$ | $(-1)x=-3$ | $(-2)x=-3$ | $\cdots$ |
| $\cdots$ | $\cdots$ | $\cdots$ | $\cdots$ | $\cdots$ | $\cdots$ | $\cdots$ |

As soluções das equações da primeira coluna são números inteiros, ou melhor, geram todos os números inteiros; as outras equações que têm solução inteira estão sublinhadas e correspondem às mesmas soluções da primeira coluna. Observe que não listamos equações do tipo $0x = a$ quando $a$ é diferente de zero, uma vez que qualquer número inteiro multiplicado por zero resulta zero: equações deste tipo não têm solução no universo dos conjuntos numéricos. As equações que restam não admitem como solução um número inteiro; são estas soluções que iremos "acrescentar" ao conjunto $\mathbb{Z}$. Mas observe que em nossa listagem de possíveis equações temos equações com a mesma solução; por exemplo, $2x = 3$ e $(-2)x = -3$. Ambas têm a mesma solução, pois a primeira se obtém da segunda pela multiplicação de um mesmo número em ambos os membros, o que não altera a equação. Assim, não será preciso acrescentar todas as soluções correspondentes às equações da tabela. Vamos listar estas equações equivalentes em colunas:

| | | | | | |
|---|---|---|---|---|---|
| $2x = 1$ | $2x = 3$ | $\cdots$ | $(-2)x = 1$ | $(-2)x = 3$ | $\cdots$ |
| $4x = 2$ | $4x = 6$ | $\cdots$ | $(-4)x = 2$ | $(-4)x = 6$ | $\cdots$ |
| $6x = 3$ | $6x = 9$ | $\cdots$ | $(-6)x = 3$ | $(-6)x = 9$ | $\cdots$ |
| $\cdots$ | $\cdots$ | $\cdots$ | $\cdots$ | $\cdots$ | $\cdots$ |
| $(-2)x = -1$ | $(-2)x = -3$ | $\cdots$ | $2x = -1$ | $2x = -3$ | $\cdots$ |
| $(-4)x = -2$ | $(-4)x = -6$ | $\cdots$ | $4x = -2$ | $4x = -6$ | $\cdots$ |
| $(-6)x = -3$ | $(-6)x = -9$ | $\cdots$ | $6x = -3$ | $6x = -9$ | $\cdots$ |
| $\cdots$ | $\cdots$ | $\cdots$ | $\cdots$ | $\cdots$ | $\cdots$ |
| $\frac{1}{2}$ | $\frac{3}{2}$ | $\cdots$ | $-\frac{1}{2}$ | $-\frac{3}{2}$ | $\cdots$ |

É claro que não podemos listar todas as possíveis equações, mas a tabela acima mostra-nos um padrão; todas as equações da primeira coluna têm a mesma solução, isto é, um número que multiplicado por $2$ resulta $1$. Este novo número será denotado $\frac{1}{2}$. Assim também acontece nas outras colunas. Cada uma delas vai gerar um novo número que não é inteiro. De modo geral, observando as duas tabelas, se a equação é $bx = a$ com $a$ e $b$ números inteiros e $b$ diferente de zero, sua solução será denotada por $\frac{a}{b}$. O conjunto resultante da ampliação que acabamos de fazer é o conjunto dos números $x$ que

são soluções de uma equação da forma $bx = a$, com $a$ e $b$ inteiros e $b$ diferente de zero. Este novo conjunto, chamado "conjunto dos números racionais" é denotado $\mathbb{Q}$.

Simbolicamente, representamos o conjunto $\mathbb{Q}$ por:

$$\mathbb{Q} = \left\{ \frac{a}{b} / \, a, b \in \mathbb{Z}, b \neq 0 \right\}.$$

**Observação 1.** Note que:

1) $\mathbb{Z} = \left\{ \frac{a}{1} / \, a \in \mathbb{Z} \right\} \subset \mathbb{Q}$, conclusão que resulta da ampliação que fizemos.

2) a natureza dos elementos de $\mathbb{Z}$ e do novo conjunto $\mathbb{Q}$ são diferentes. Por este motivo não poderíamos afirmar que $\mathbb{Z} \subset \mathbb{Q}$. No entanto, como podemos identificar $\mathbb{Z}$ como um subconjunto de $\mathbb{Q}$, usamos $\mathbb{Z} \subset \mathbb{Q}$. Veremos logo a seguir que a estrutura de $\mathbb{Z}$ (operações, propriedades e ordem) se mantém nesta nova representação.

**Observação 2.** Na representação $\frac{a}{b}$ de um número racional, $a$ é o **numerador** e $b$ é o **denominador.**

**Observação 3.** Note que um número racional $\frac{a}{b}$ é igual a zero quando seu numerador é igual a zero.

## Tarefa

Pesquise qual a origem das palavras *numerador* e *denominador.*

**Comentários:**

1) **Sobre frações como parte de um todo.** De modo geral, o primeiro contato dos alunos com os números racionais se dá através da idéia de **fração**, como uma quantidade que representa uma parte do todo. O universo de trabalho neste nível é o conjunto dos números naturais, e "divisão" significa divisão exata (o algoritmo da divisão com resto zero).

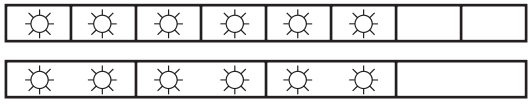
**Alguns exemplos**

a) $\frac{1}{2}$ maçã representa a quantidade correspondente a um dos pedaços que resulta da divisão da maçã em *duas* partes iguais.

b) $\frac{1}{3}$ de 30 balas representa a quantidade correspondente a *um* dos "pedaços" que resulta da divisão de 30 por *três*, ou seja, 10 balas.

c) $\frac{2}{5}$ de 100 reais representa a quantidade correspondente a dois dos pedaços que resulta da divisão de 100 reais por 5, ou seja, $2.(100 \div 5) = 2.20 = 40$ reais.

**2) Sobre frações equivalentes**. Os números racionais $\frac{3}{4}$ e $\frac{6}{8}$ provêm das equações $4x = 3$ e $8x = 6$ respectivamente. Como $8x = 6$ resulta da multiplicação por 2 em ambos os membros de $4x = 3$, $\frac{3}{4}$ e $\frac{6}{8}$ são *duas representações do mesmo número racional*. Note que $\frac{6}{8}$ se obtém de $\frac{3}{4}$ pela multiplicação por 2 do numerador e do denominador; $\frac{6}{8}$ e $\frac{3}{4}$ são *frações equivalentes.* Pensando em uma fração como parte de um todo, dividir o todo em 4 partes iguais e tomar 3 resulta na mesma quantidade obtida se dividirmos o todo em 8 partes iguais e tomarmos 6. Veja o clássico desenho que aparece nos livros didáticos:



Outras representações do número racional $\frac{3}{4}$ são: $\frac{-3}{-4}$, $\frac{12}{16}$, $\frac{9}{12}$, etc.

Você deve ter percebido que um número racional tem então uma infinidade de representações; podemos escolher trabalhar com aquela que for mais adequada, dependendo da situação. Por exemplo, se

temos o número $\frac{5}{9}$ e necessitamos trabalhar com denominador $45$, podemos substituir $\frac{5}{9}$ por $\frac{5.5}{5.9}=\frac{25}{45}$ pois $\frac{5}{9}=\frac{25}{45}$.

### Exercícios propostos

1) Subtraindo-se um mesmo número do numerador e do denominador da fração $\frac{8}{12}$, obtém-se uma fração equivalente a $\frac{8}{12}$?

2) Desenhe um segmento de $12$ cm de comprimento e marque os números de zero a $12$. Associe cada uma das frações seguintes a um ponto do segmento: $\frac{3}{4}$ de $12$, $\frac{5}{6}$ de $12$, $\frac{7}{14}$ de $12$, $\frac{2}{24}$ de $12$ e $\frac{1}{4}$ de $12$.

3) Que fração da hora é o minuto? Quantos minutos há em $\frac{3}{5}$ de hora?

4) Quantos meios litros há em $5$ litros e meio?

5) Existe uma fração equivalente a um terço com denominador $10$?

6) Soma-se $7$ ao denominador da fração $\frac{2}{14}$. Quanto se deve somar ao numerador para obter uma fração equivalente?

## 6.3 Operações em $\mathbb{Q}$

Para definir as operações em $\mathbb{Q}$, usaremos as operações em $\mathbb{Z}$ e suas propriedades (capítulo 2), propriedades estas que não gostaríamos de "perder" no processo de ampliação. Considerar um número racional como solução de uma equação nos permite encontrar uma maneira de operar os novos números de modo que a estrutura de $\mathbb{Z}$ se mantém também em $\mathbb{Q}$. É como se fizéssemos o processo de operar "de trás para frente": considerando que as propriedades de $\mathbb{Z}$ se mantêm em $\mathbb{Q}$, como posso operar com os novos números?

### 6.3.1 Adição em $\mathbb{Q}$

Consideramos dois números racionais $x$ e $y$. Como os elementos do conjunto $\mathbb{Q}$ são soluções de equações, temos que existem $a, b, c$ e $d$ inteiros, $b$ e $d$ não nulos, tais que

1) $x$ é solução de $bx = a$

e

2) $y$ é solução de $dy = c$.

**Pergunta:** qual a equação que tem $x + y$ como solução? Ou seja, para quais inteiros $p + q$, com $q \neq 0$, temos $q(x + y) = p$? Multiplicando ambos os membros da equação 1) por $d$ e ambos os membros da equação 2) por $b$, e considerando que estão mantidas as propriedades associativa, comutativa e distributiva em $\mathbb{Q}$ (pois $x$ e $y$ são racionais), obtemos:

3) $bdx = ad$ e

4) $bdy = bc$

**Adicionando membro a membro temos:**

$$bdx + bdy = ad + bc$$
$$bd(x + y) = ad + bc$$

Assim, $x + y$ é solução da equação $bd(x + y) = ad + bc$. Os inteiros que estávamos procurando são $q = bd \neq 0$ (pois $b$ e $d$ são não nulos), e $p = ad + bc$, ou seja, $x + y$ é solução da equação $(bd)(x + y) = ad + bc$ e é representado em $\mathbb{Q}$ como $\frac{ad + bc}{bd}$. Isto nos indica como definir a adição em $\mathbb{Q}$:

**Definição.** Dados dois números racionais $\frac{a}{b}$ e $\frac{c}{d}$, com $a, b, c$ e $d$ inteiros, $b \neq 0$ e $d \neq 0$, definimos sua soma como:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}.$$

**Observação 4.** Nesta soma de frações não estranhe o fato de não precisarmos do *mmc* dos denominadores. Acompanhe os exemplos a seguir.

**Exemplos**

4) $\frac{3}{8}+\frac{13}{6}=\frac{3.6+8.13}{8.6}=\frac{18+104}{48}=\frac{122}{48}$.

Se a soma for feita com o *mmc* dos denominadores $8$ e $6$, teremos: *mmc* $(8,6)=24$ e as frações equivalentes com denominador 24 são $\frac{3.3}{8.3}=\frac{9}{24}$ e $\frac{13.4}{6.4}=\frac{52}{24}$.

Então $\frac{3}{8}+\frac{13}{6}=\frac{9}{24}+\frac{52}{24}=\frac{61}{24}$.

Como $\frac{61}{24}=\frac{122}{48}$, pois $61.2=122$ e $24.2=48$, obtemos o mesmo resultado.

5) $\frac{3}{17}+\frac{7}{17}=\frac{3.17+7.17}{17.17}=\frac{17.(3+7)}{17.17}=\frac{10}{17}$.

Observe que na última igualdade estamos usando o fato de que as frações $\frac{17.10}{17.17}$ e $\frac{10}{17}$ são equivalentes. Observe também que, como os denominadores das frações que queremos somar são iguais, basta somar os numeradores e considerar o mesmo denominador.

6) $3+\frac{6}{7}=\frac{3}{1}+\frac{6}{7}=\frac{3.7+1.6}{1.7}=\frac{27}{7}$.

(Observe que para efetuar o algoritmo da adição em $\mathbb{Q}$ precisamos representar o número inteiro $3$ como $\frac{3}{1}$).

Um número como $3+\frac{6}{7}$ pode ser anotado por $3\frac{6}{7}$ e é chamado um número misto. De modo geral se $q$, $a$ e $b$ são inteiros, o número $q\frac{a}{b}$ representa a soma $q+\frac{a}{b}$.

**Propriedades da adição em $\mathbb{Q}$**

Assim como em $\mathbb{Z}$, a adição de números racionais é associativa e comutativa (propriedades A1 e A2). $\mathbb{Q}$ também possui as proprie-

dades da existência do elemento neutro e da existência do oposto, que vamos detalhar a seguir. Assim, em relação à adição, $\mathbb{Q}$ admite as mesmas propriedades que $\mathbb{Z}$.

A3) Para todo número racional $\frac{a}{b}$ (com $a$ e $b$ inteiros e $b \neq 0$), existe o número racional $\frac{0}{1}$ tal que $\frac{a}{b}+\frac{0}{1}=\frac{a}{b}$.

**Demonstração.** O "candidato" a ser o elemento neutro da adição em $\mathbb{Q}$ é o número inteiro $0$, que em $\mathbb{Q}$ é representado por $\frac{0}{1}$ (poderíamos ter escolhido qualquer outro denominador, mas $1$ é o mais conveniente neste caso; lembre das frações equivalentes!). Vamos verificar que ele satisfaz a condição: $\frac{a}{b}+\frac{0}{1}=\frac{a.1+b.0}{b.1}=\frac{a+0}{b}=\frac{a}{b}$. (Note que usamos as propriedades das operações em $\mathbb{Z}$ no numerador).

Anotaremos o elemento neutro $\frac{0}{1}$ por $0$, como em $\mathbb{Z}$.

■

A4) Para todo número racional $\frac{a}{b}$ (com $a$ e $b$ inteiros e $b \neq 0$), existe um número racional $\frac{r}{s}$ tal que $\frac{a}{b}+\frac{r}{s}=0$.

**Demonstração.** Estamos procurando um número racional $\frac{r}{s}$ que somado com $\frac{a}{b}$ resulte zero; observemos que:

$$\frac{a}{b}+\frac{r}{s}=\frac{a.s+b.r}{b.s}=\frac{0}{1}.$$

Mas a última igualdade ocorre quando $a.s+b.r=0$, ou seja, quando $a.s$ e $b.r$ são opostos. Como $\frac{a}{b}$ é o número dado, quais valores deverão tomar $s$ e $r$ para que $a.s=-(b.r)$? Fazendo $s=b$ e $r=-a$ obtemos: $a.b=-[b.(-a)]$, uma afirmação verdadeira pelas propriedades das operações em $\mathbb{Z}$ (verifique!). Assim, o oposto de $\frac{a}{b}$ em $\mathbb{Q}$ é $\frac{-a}{b}=-\frac{a}{b}$. Note que $\frac{a}{-b}$ também pode ser o oposto de $\frac{a}{b}$, uma vez que $\frac{-a}{b}=\frac{a}{-b}$ (por quê?).

■

## 6.3.2 Subtração em $\mathbb{Q}$

A subtração em $\mathbb{Q}$ é definida como em $\mathbb{Z}$: subtrair é somar o oposto.

**Definição.** Dados dois números racionais $\frac{a}{b}$ e $\frac{c}{d}$, com $a$, $b$, $c$ e $d$ inteiros, com $b \neq 0$ e $d \neq 0$, definimos sua diferença como:

$$\frac{a}{b} - \frac{c}{d} = \frac{a}{b} + (-\frac{c}{d}) = \frac{ad - bc}{bd}.$$

**Exemplos**

7) $\frac{4}{9} - \frac{5}{6} = \frac{4}{9} + (-\frac{5}{6}) = \frac{4}{9} + (\frac{-5}{6}) = \frac{4.6 - 9.5}{9.6} = \frac{24 - 45}{54} = \frac{-21}{54} = -\frac{21}{54}$.

8) $7 - \frac{3}{8} = \frac{7}{1} - \frac{3}{8} = \frac{7.8 - 3.1}{1.8} = \frac{56 - 3}{8} = \frac{53}{8}$.

9) $\frac{7}{4} - \frac{5}{4} = \frac{7 - 5}{4} = \frac{2}{4}$.

## Exercícios propostos

7) Uma piscina é enchida por duas torneiras. A primeira, sozinha, encheria a piscina em 2 horas, e a segunda, em 5 horas. Que fração do tanque é enchida pelas duas torneiras em uma hora?

8) Numa receita de biscoitos, os ingredientes são:

- um décimo de quilo de açúcar;
- um quinto de quilo de margarina;
- um quarto de quilo de farinha de trigo.

Qual o peso total dos ingredientes para uma receita? Quanto será necessário de cada ingrediente para duas receitas? Qual a massa total dos ingredientes para duas receitas?

9) A quadra de vôlei tem $20\frac{1}{2}$ metros de comprimento por $12\frac{3}{4}$ metros de largura. Quantos metros a mais tem o comprimento em relação à largura?

10) Quanto se deve subtrair de cada uma das frações $\frac{5}{3}, \frac{18}{13}, \frac{7}{4}, \frac{8}{5}$ para se obter um inteiro?

11) Lígia saiu de casa às 8 horas e 15 minutos. Levou meia hora para chegar à escola, teve 3 aulas de quatro quintos de hora e telefonou para sua mãe buscá-la na escola. A que horas Lígia telefonou, sabendo que ela ligou imediatamente após a terceira aula?

## 6.3.3 Multiplicação em $\mathbb{Q}$

Consideramos dois números racionais $x$ e $y$. Da mesma forma como fizemos para a adição, temos que existem $a$, $b$, $c$ e $d$ inteiros, $b$ e $d$ não nulos, tais que:

1) $x$ é solução de $bx = a$ e

2) $y$ é solução de $dy = c$.

**Pergunta:** qual a equação que tem $x.y$ como solução? Ou seja, para quais inteiros $p$ e $q$, com $q \neq 0$, temos $q(x.y) = p$? Multiplicando membro a membro as equações 1) e 2) e considerando que as propriedades associativa e comutativa se mantêm em $\mathbb{Q}$ (pois $x$ e $y$ são racionais), obtemos:

$$(bx).(dy) = a.c$$
$$bd(xy) = ac.$$

Esta é a equação cuja solução é $x.y$; o produto $x.y$ será representado em $\mathbb{Q}$ por $\frac{ac}{bd}$. Podemos então definir:

**Definição.** Dados dois números racionais $\frac{a}{b}$ e $\frac{c}{d}$, com $a$, $b$, $c$ e $d$ inteiros, $b$ e $d$ não nulos, definimos seu produto como:

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

**Exemplos**

10) $\frac{7}{11} \cdot \frac{4}{9} = \frac{7.4}{11.9} = \frac{28}{99}$.

11) $3 \cdot \frac{1}{4} = \frac{3}{1} \cdot \frac{1}{4} = \frac{3}{4}$.

12) $\frac{5}{1}\cdot\frac{7}{1}=\frac{5.7}{1}=\frac{35}{1}=35$.

O exemplo 12 nos mostra que, ao multiplicarmos em $\mathbb{Q}$ dois números inteiros, o resultado é ainda um número inteiro.

**Propriedades da multiplicação em $\mathbb{Q}$**

Assim como em $\mathbb{Z}$, a multiplicação de números racionais é associativa e comutativa (propriedades M1 e M2). $\mathbb{Q}$ também possui a propriedade da existência de elemento neutro para a multiplicação. Além disso, com a ampliação, ganhamos uma nova propriedade: a existência do elemento inverso. Vamos detalhar a seguir estas duas propriedades:

M3) **Existência do elemento neutro.** Existe um número racional $\frac{r}{s}$ tal que $\frac{r}{s}\cdot\frac{a}{b}=\frac{a}{b}$, para todo número racional $\frac{a}{b}$.

**Demonstração.** É razoável pensar que o elemento neutro de $\mathbb{Q}$ para a multiplicação será o mesmo de $\mathbb{Z}$, como aconteceu na adição. Escolhemos para $1$ a representação $\frac{1}{1}$. Lembre-se que existe uma infinidade de representações para o inteiro $1$: $\frac{1}{1}, \frac{2}{2}, \frac{-5}{-5}, \cdots$. Toda fração da forma $\frac{k}{k}$ para $k$ inteiro não nulo é uma representação do inteiro $1$. Vamos verificar o que ocorre:

$$\frac{1}{1}\cdot\frac{a}{b}=\frac{1.a}{1.b}=\frac{a}{b}.$$

■

Observe que o inteiro $1$ fez o seu papel de elemento neutro (em $\mathbb{Z}$) no numerador e no denominador. Assim, o elemento neutro de $\mathbb{Q}$ para a multiplicação é $\frac{1}{1}$ que anotaremos como $1$.

A propriedade que vamos estabelecer a seguir não ocorre em $\mathbb{Z}$. Quando ampliamos $\mathbb{Z}$, "ganhamos" mais uma propriedade para a multiplicação, que irá fornecer a $\mathbb{Q}$ uma nova estrutura (diferente de $\mathbb{Z}$) e que nos permitirá definir uma nova operação (a divisão). A propriedade nos diz que, para todo número racional não nulo $x$, existe um racional $y$ tal que $x.y=1$; $y$ é chamado o *inverso* de $x$.

Observe que este fato só ocorre em $\mathbb{Z}$ quando $x = y = 1$ ou $x = y = -1$.

M4) **Existência do elemento inverso.** Para todo número racional não nulo $\frac{a}{b}$, existe um número racional $\frac{c}{d}$ tal que $\frac{a}{b} \cdot \frac{c}{d} = 1$.

**Demonstração.** Antes de iniciar a demonstração vamos fazer algumas "experiências":

1) Para o racional $\frac{5}{8}$: qual o número racional $\frac{c}{d}$ que multiplicado por $\frac{5}{8}$ resulta 1?

   Para que ocorra $\frac{5}{8} \cdot \frac{c}{d} = 1$, devemos ter $\frac{5.c}{8.d} = 1$, ou seja, as frações $\frac{5.c}{8.d}$ *e* $\frac{1}{1}$ são equivalentes. Mas as frações equivalentes a $\frac{1}{1}$ são aquelas cujo numerador é igual ao denominador; então teremos $5.c = 8.d$, com $c$ e $d$ números inteiros. Esta igualdade ocorre para $c = 8$ e $d = 5$. Assim, o inverso de $\frac{5}{8}$ em $\mathbb{Q}$ é o número $\frac{8}{5}$.

2) Para o racional $9 = \frac{9}{1}$, seu inverso será $\frac{1}{9}$, uma vez que $9 \cdot \frac{1}{9} = \frac{9}{9} = 1$.

Você já deve ter percebido o que está acontecendo. Vamos formalizar a idéia fazendo a demonstração, isto é, exibindo um número racional que multiplicado por $\frac{a}{b}$ resulte 1.

De fato: considere o racional não nulo $\frac{a}{b}$. Sabemos que $a$ e $b$ são inteiros e que $b \neq 0$; como o racional é não nulo, também teremos $a \neq 0$. Isto nos permite afirmar que $\frac{b}{a}$ é um número racional, também não nulo. Assim, $\frac{b}{a}$ é nosso candidato a ser o inverso de $\frac{a}{b}$. Vamos verificar:

$$\frac{a}{b} \cdot \frac{b}{a} = \frac{a.b}{b.a} = \frac{a.b}{a.b} = 1.$$

Desta forma, o inverso de $\frac{a}{b}$ é $\frac{b}{a}$.

■

**Notação.** Denotamos o inverso de $\frac{a}{b}$ por $\left(\frac{a}{b}\right)^{-1}$, isto é, $\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$.

**Observação 5.** Note que o inverso de um número racional existe se, e somente se, o racional é não nulo!

Vamos agora definir uma nova operação em $\mathbb{Q}$: a divisão. Note que o Algoritmo da Divisão que estudamos no capítulo 3 não era uma operação em $\mathbb{Z}$, mas uma relação entre dois números inteiros.

### 6.3.4 Divisão em $\mathbb{Q}$

Dados os números racionais, $\frac{a}{b}$ e $\frac{p}{q}$ com $\frac{p}{q} \neq 0$, definimos:

$$\frac{a}{b} \div \frac{p}{q} = \frac{a}{b} \cdot \left(\frac{p}{q}\right)^{-1} = \frac{a}{b} \cdot \frac{q}{p} = \frac{aq}{bp}.$$

**Exemplos**

13) $\frac{5}{13} \div \frac{7}{4} = \frac{5}{13} \cdot \frac{4}{7} = \frac{20}{91}$.

14) $\frac{1}{4} \div 3 = \frac{1}{4} . \frac{1}{3} = \frac{1}{12}$.

15) $3 \div \frac{1}{2} = \frac{3}{1} \div \frac{1}{2} = \frac{3}{1} \cdot \frac{2}{1} = \frac{6}{1} = 6$.

**Observação 6.** A operação divisão não é associativa, não é comutativa e não possui elemento neutro. Note que, assim como subtrair é "somar o oposto", dividir é "multiplicar pelo inverso".

## 6.4 Frações irredutíveis

Você já sabe que cada número racional possui uma infinidade de representações na forma de frações. Mas uma delas é especial, e bastante conveniente em muitos casos: são as chamadas frações irredutíveis.

**Definição.** Sejam $a$ e $b$ números inteiros com $b$ diferente de zero. Uma fração $\frac{a}{b}$ é irredutível quando $mdc\ (a,b)=1$.

O resultado a seguir nos diz que todo número racional possui uma representação na forma de fração irredutível.

**Teorema.** Todo número racional $x$ pode ser expresso na forma $\frac{a}{b}$ com $mdc\ (a,b)=1$.

**Demonstração.**

Seja $x$ um número racional na forma $\frac{r}{s}$, com $r$ e $s$ inteiros e $s\neq 0$. Como $r$ e $s$ são inteiros, existe o $mdc\ (r,s)$, que chamaremos $d$, e existem $a$ e $b$ inteiros, $b\neq 0$, tais que $r=d.a$, $s=d.b$ e $mdc\ (a,b)=1$. Então

$$\frac{r}{s}=\frac{d.a}{d.b}=\frac{d}{d}\cdot\frac{a}{b}=1\cdot\frac{a}{b}=\frac{a}{b}.$$

Logo a representação irredutível de $\frac{r}{s}$ é $\frac{a}{b}$.

■

**Observação 7.** A demonstração do teorema nos ensina como encontrar a representação irredutível de um número racional. Veja um exemplo: qual a representação na forma de fração irredutível do racional $\frac{32}{20}$? Fazemos inicialmente $mdc\ (32,20)=4$ (se você esqueceu como calcular o $mdc$ volte ao capítulo 3 ). Então $32=4.8$ e $20=4.5$, com $mdc\ (8,5)=1$. Assim a fração irredutível equivalente a $\frac{32}{20}$ é $\frac{8}{5}$, ou seja, $\frac{32}{20}=\frac{8}{5}$.

## 6.5 Sobre a simplificação de frações

"Simplificar uma fração" é encontrar sua forma irredutível; de modo geral não calculamos o $mdc$; vamos eliminando os fatores comuns até que não seja mais possível. Por exemplo, para $\frac{32}{20}$, fazemos: $\frac{32}{20}=\frac{2.16}{2.10}=\frac{16}{10}=\frac{2.8}{2.5}=\frac{8}{5}$. Este procedimento está correto, pois o que

fizemos foi "eliminar" o maior fator comum dos dois números (o *mdc*), resultando na fração irredutível. No entanto, simplificar uma fração não é um procedimento "obrigatório": não podemos dizer que um estudante errou a questão se sua resposta for $\frac{36}{14}$, um racional que não é irredutível. Se o professor deseja que o estudante "simplifique" a fração, ele deve dizer explicitamente: "dê a solução em sua forma irredutível". Não podemos esquecer que $\frac{36}{14}$ e $\frac{18}{7}$ são representações do mesmo número racional.

## 6.6 Sobre a nomenclatura das frações

É comum nos livros didáticos aparecerem nomes especiais para certos tipos de frações; vamos explicitar alguns deles:

1) Fração própria: $\frac{a}{b}$ quando $a < b$. Exemplos: $\frac{1}{5}, \frac{8}{14}, \frac{45}{123}$.
2) Fração imprópria: $\frac{a}{b}$ quando $b < a$. Exemplos: $\frac{4}{3}, \frac{7}{2}, \frac{456}{120}$.
3) Fração decimal: quando o denominador é potência de $10$. Exemplos: $\frac{3}{10}, \frac{9}{100}, \frac{56}{1000}$.
4) Fração aparente: quando o numerador é múltiplo do denominador. Exemplos: $\frac{30}{5}, \frac{450}{50}, \frac{98}{7}$.
5) Fração unitária: quando o numerador é $1$. Exemplos: $\frac{1}{10}, \frac{1}{110}, \frac{1}{56}$.

### Exercícios propostos

12) Quanto é a terça parte de um meio?

13) Numa sala há $20$ alunos. Hoje estão presentes três quartos dos alunos da classe e, dos presentes, dois quintos irão ao zoológico. Quantos alunos estão presentes hoje? Quantos irão ao zoológico?

14) Uma jarra tem a capacidade de dois terços de litro. Quando a jarra estiver cheia até sua metade com suco, quantos litros conterá?

15) Num mapa da cidade, 1 cm representa 10 quilômetros. Uma distância de $1\frac{3}{5}$ cm no mapa corresponde a quantos quilômetros?

16) Uma garrafa contém dois terços de litro. Quantos litros contêm 9 garrafas iguais a esta?

17) Qual o número que multiplicando por dois quintos resulta como produto sete oitavos?

18) Quantos centésimos tem um décimo?

19) Quantos cinco décimos há em 8 inteiros?

20) Um tanque contendo 750 litros de água está apenas com seis décimos de sua capacidade. Quantos litros de água haveria no tanque se estivesse cheio? Quanto falta para enchê-lo?

21) O que é mais barato: 6 laranjas por 0,34 reais ou 8 laranjas por 0,41 reais?

22) Se um piloto corre a 200 Km/h, quantos metros percorre num segundo, supondo que sua velocidade seja constante?

23) Dos $\frac{3}{4}$ restantes de um bolo, comi $\frac{2}{3}$. Que fração do bolo comi?

24) Que fração devo somar a $\frac{2}{3}$ para obter $\frac{8}{9}$?

25) Qual o número que multiplicado por $\frac{1}{3}$ resulta, como produto, $\frac{3}{5}$?

26) Quanto se deve subtrair de $\frac{2}{3}$ para se obter a terça parte de $\frac{3}{5}$?

27) Uma peça de fazenda, depois de molhada, encolheu $\frac{2}{15}$ de seu comprimento, ficando com $39$ metros. Quantos metros tinha esta peça antes de encolher?

28) Imagine um recipiente de um litro ocupado até seus $\frac{2}{3}$ com guaraná. Supondo que se queira distribuir esse guaraná em copos, cuja capacidade é $\frac{1}{5}$ de litro, quantos copos ficarão cheios e que fração de copo sobrará?

29) Quantos oito décimos há em $16$ inteiros?

30) A fortuna de João foi dividida da seguinte forma: um quinto para seu irmão mais velho, um sexto do restante para seu irmão mais novo e partes iguais para cada um de seus $12$ filhos. Que fração da fortuna cada filho recebeu? Dê a resposta na forma irredutível.

31) Em um mapa, um centímetro representa dezesseis quilômetros. Qual a distância real representada por cinco centímetros e meio?

32) Mostre com exemplos que a divisão não é associativa e não é comutativa. Mostre também que não vale a propriedade distributiva da divisão em relação à adição.

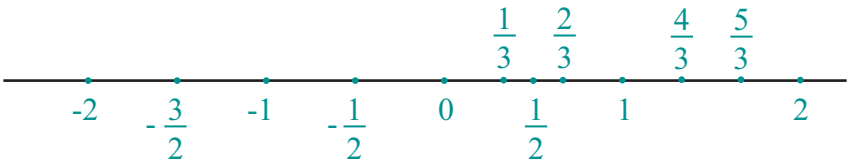
33) Expresse em frações irredutíveis cada uma das expressões:

a) $10^{-1}+15^{-2}+6.7^{-1}+(4.8)^{-1}$

b) $4^{-3}+5.10^{-1}+7.14^{-2}+(8+5)^{-1}$.

# 6.7 Relação de ordem em $\mathbb{Q}$

Como comparar números racionais? Por exemplo: quem é maior, $\frac{4}{5}$ ou $\frac{5}{6}$? Vamos marcar sobre a reta alguns números racionais:




As frações unitárias (com numerador igual a 1) são partes de um inteiro e estão entre zero e 1. Para outros racionais não inteiros, utiliza-se a mesma idéia dos múltiplos em $\mathbb{Z}$: $\frac{2}{3}$ é $2.\frac{1}{3}$ ou ainda, dois "pedaços" de $\frac{1}{3}$. Generalizando, um número $\frac{a}{b}$ corresponde a "$a$ pedaços de $\frac{1}{b}$".

Nosso objetivo é ampliar a relação de ordem que já tínhamos em $\mathbb{Z}$, "acrescentando" os racionais não inteiros na reta, mantendo a ordem dos inteiros.

A relação de ordem em $\mathbb{Q}$ será definida levando em conta o fato de que já conhecemos os números inteiros positivos: $\mathbb{Z}_+^* = \{1, 2, 3, \ldots\}$.

**Definição.** Um número racional $\frac{a}{b}$ é positivo quando $a.b$ é um número inteiro positivo.

**Observação 8.** Lembre-se dos resultados já estudados no capítulo 2:

i) O produto $a.b$ é positivo quando $a > 0$ e $b > 0$ ou quando $a < 0$ e $b < 0$.

ii) O produto $a.b$ é negativo quando $a > 0$ e $b < 0$ ou $a < 0$ e $b > 0$.

iii) O produto $a.b$ é zero quando $a = 0$ ou $b = 0$.

Fazendo uma analogia com os inteiros, temos:

- Um número racional $\frac{a}{b}$ é não positivo quando $a.b < 0$ ou $a.b = 0$.

- Um número racional $\frac{a}{b}$ é negativo quando $a.b < 0$.
- Um número racional $\frac{a}{b}$ é não negativo quando $a.b > 0$ ou $a.b = 0$.

Podemos então definir em $\mathbb{Q}$ o conjunto dos "racionais positivos", $\mathbb{Q}_+^* = \left\{ \frac{a}{b} / \, a.b > 0 \right\}$. Os axiomas de ordem são os seguintes:

AO1) As operações de adição e multiplicação são fechadas em $\mathbb{Q}_+^*$, ou seja: se $x$ e $y$ são racionais positivos, então $x + y$ e $x.y$ são racionais positivos.

AO2) Se $x$ é um número racional, então $x \in \mathbb{Q}_+^*$ ou $-x \in \mathbb{Q}_+^*$ ou $x = 0$ (este "ou" é exclusivo).

**Observação 9.** Note que a igualdade dos racionais $\frac{-a}{b}$ e $\frac{a}{-b}$ nos permite escrever qualquer número racional $\frac{a}{b}$ com denominador positivo. Assim, o conjunto dos números racionais pode ser expresso por $\mathbb{Q} = \left\{ \frac{a}{b} / \, a, b \in \mathbb{Z} \text{ e } b > 0 \right\}$. Considerando esta representação do conjunto $\mathbb{Q}$, podemos dizer que um número racional $\frac{a}{b}$ é positivo quando $a > 0$.

**Definição.** Dados dois números racionais $x$ e $y$ definimos:

i) $x \leq y$ quando $y - x \in \mathbb{Q}_+$ ($y - x$ é não negativo).

ii) $x < y$ quando $y - x \in \mathbb{Q}_+^*$ ($y - x$ é positivo).

**Observação 10.** Como expressar relação $x \leq y$ fazendo $x = \frac{a}{b}$ e $y = \frac{c}{d}$, com $b > 0$ e $d > 0$?

Acompanhe com atenção:

$x \leq y$ quando $y - x \in \mathbb{Q}_+$

$\frac{a}{b} \leq \frac{c}{d}$ quando $\frac{c}{d} - \frac{a}{b} = \frac{bc - ad}{bd} \in \mathbb{Q}_+$

$\frac{bc-ad}{bd} \in \mathbb{Q}_+$ quando $bc-ad \geq 0$ em $\mathbb{Z}$, ou seja, $ad \leq bc$.

Logo, podemos dizer que $\frac{a}{b} \leq \frac{c}{d}$ quando $ad \leq bc$.

Exemplo: $\frac{3}{4} \leq \frac{5}{6}$ pois $3.6 = 18 \leq 4.5 = 20$.

**Observação 11.** Outra maneira de comparar as frações é reduzi-las ao mesmo denominador, usando as frações equivalentes. Por exemplo, podemos escrever $\frac{3}{4}$ e $\frac{5}{6}$ como $\frac{9}{12}$ e $\frac{10}{12}$; então $\frac{9}{12} \leq \frac{10}{12}$, pois $9 \leq 10$, ou seja, $\frac{3}{4} \leq \frac{5}{6}$.

**Observação 12**. Assim como em $\mathbb{Z}$, podemos definir a relação $<$ da seguinte maneira:

Para $x$ e $y$ racionais, $x < y$ se e somente se $x \leq y$ *e* $x \neq y$.

Isto é equivalente a: $x < y$ quando $y - x \in \mathbb{Q}_+^*$.

## 6.7.1 Propriedades da relação de ordem

Valem em $\mathbb{Q}$ as mesmas propriedades da relação de ordem em $\mathbb{Z}$:

**Proposição 1.** A relação $\leq$ em $\mathbb{Q}$ as possui as seguintes propriedades:

i) Reflexiva: $x \leq x$, para todo número racional $x$.

ii) Anti-simétrica: se $x \leq y$ e $y \leq x$ então $x = y$, para quaisquer números racionais $x$ e $y$.

iii) Transitiva: se $x \leq y$ e $y \leq z$, então $x \leq z$, para quaisquer números racionais $x, y$ e $z$.

**Demonstração.** O procedimento é o mesmo da demonstração em $\mathbb{Z}$. Faça como exercício.

**Proposição 2.** Para quaisquer números racionais $x$, $y$, $z$ e $w$, tem-se:

a) $x \leq y$ se, e somente se, $x + z \leq y + z$.

b) Se $x \leq y$ e $0 \leq z$ então $xz \leq yz$.

c) Se $x \leq y$ e $z < 0$ então $yz \leq xz$.

d) Se $x \leq y$ e $z \leq w$ então $x + z \leq y + w$.

e) $x \leq y$ se, e somente se, $-y \leq -x$.

**Demonstração.** Como o procedimento também aqui é o mesmo feito em $\mathbb{Z}$, faça a demonstração como exercício.

**Observação 13.** Quais das afirmações da Proposição 2 continuam verdadeiras se substituirmos $\leq$ por $<$? a), b) e c) afirmam que $\leq$ é compatível com as operações de adição e multiplicação em $\mathbb{Q}$ e o mesmo ocorre para a relação $<$. As afirmações d) e c) também continuam verdadeiras para $<$.

**Proposição 3.** Para quaisquer $x$ e $y$ racionais não nulos, tem-se:

1) i) Se $x > 0$ então $x^{-1} > 0$.

ii) Se $x < 0$ então $x^{-1} < 0$.

**Demonstração.**

i) Se $x > 0$ e $x.x^{-1} = 1 > 0$, $x^{-1}$ deve ser positivo, uma vez que o produto de dois racionais é positivo quando ambos são positivos ou ambos são negativos.

ii) Analogamente, se $x < 0$ e $x.x^{-1} = 1 > 0$, $x^{-1}$ deve ser negativo.

■

2) i) Se $0 < x < 1$ então $x^{-1} > 1$.

ii) Se $x > 1$ então $x^{-1} < 1$.

**Demonstração.**

i) Se $0 < x < 1$, teremos $x > 0$ e por (1) $x^{-1} > 0$. Multiplicando ambos os membros da desigualdade $x < 1$ por $x^{-1}$, obtemos $x.x^{-1} < 1.x^{-1}$, ou seja, $x^{-1} > 1$.

ii) Se $x > 1$, temos $x > 0$ e por (1) $x^{-1} > 0$. Multiplicando ambos os membros da desigualdade $x > 1$ por $x^{-1}$, obtemos $x.x^{-1} > 1.x^{-1}$, ou seja, $x^{-1} < 1$. Como $x^{-1} > 0$, podemos concluir que $0 < x^{-1} < 1$.

■

3) i) Se $0 < x < y$ então $0 < y^{-1} < x^{-1}$.

ii) Se $x < y < 0$ então $y^{-1} < x^{-1} < 0$.

**Demonstração.**

i) Se $x$ e $y$ são positivos, então por (1), $x^{-1}$ e $y^{-1}$ também são positivos. Multiplicando ambos os membros da desigualdade $x < y$ pelo número positivo $(x^{-1}.y^{-1})$ obtemos:

$$x^{-1}.y^{-1}.x < x^{-1}.y^{-1}.y$$
$$(x^{-1}.x).y^{-1} < x^{-1}.(y^{-1}.y)$$
$$1.y^{-1} < x^{-1}.1$$
$$y^{-1} < x^{-1}$$
$$0 < y^{-1} < x^{-1}.$$

ii) Se $x$ e $y$ são negativos, também $x^{-1}$ e $y^{-1}$ são negativos (por 1). Logo, o produto $x^{-1}.y^{-1}$ é positivo. Multiplicando ambos os membros da desigualdade $x < y$ por $(x^{-1}.y^{-1})$, obtemos:

$$x^{-1}.y^{-1}.x < x^{-1}.y^{-1}.y$$
$$(x^{-1}.x).y^{-1} < x^{-1}.(y^{-1}.y)$$
$$1.y^{-1} < x^{-1}.1$$
$$y^{-1} < x^{-1}$$
$$y^{-1} < x^{-1} < 0.$$

■

## 6.8 Valor absoluto (ou módulo)

A definição é a mesma dos inteiros: para $x$ um número racional,

$$|x| = \begin{cases} x \ se \ x \geq 0 \\ -x \ se \ x < 0 \end{cases}.$$

As propriedades que valiam em $\mathbb{Z}$ também valem em $\mathbb{Q}$. Além disso, se $x$ é um número racional na forma $\frac{a}{b}$, temos que $|\frac{a}{b}| = \frac{|a|}{|b|}$. Prove!

## 6.9 Densidade

Dados dois números racionais diferentes, é sempre possível encontrar outro número racional entre eles; na verdade, é possível encontrar uma infinidade de números racionais entre eles! Vamos observar algumas situações:

$$\frac{1}{2} < \frac{2}{3} \ .$$

O ponto médio entre $\frac{1}{2}$ e $\frac{2}{3}$ é o número racional

$$z_1 = \frac{1}{2} \cdot \left( \frac{1}{2} + \frac{2}{3} \right) = \frac{1}{2} \cdot \frac{5}{6} = \frac{5}{12} .$$

Assim, $\frac{1}{2} < \frac{5}{12} < \frac{2}{3}$.

Considerando agora os racionais $\frac{5}{12}$ e $\frac{2}{3}$, achamos o ponto médio entre eles:

$$z_2 = \frac{1}{2} \cdot \left( \frac{5}{12} + \frac{2}{3} \right) = \frac{1}{2} \cdot \frac{13}{12} = \frac{13}{24} .$$

Assim, $\frac{5}{12} < \frac{13}{24} < \frac{2}{3}$.

Considerando agora os racionais $\frac{13}{24}$ e $\frac{2}{3}$, achamos o ponto médio entre eles, que será $\frac{29}{48}$ (faça as contas!). Continuando com este procedimento, encontramos uma infinidade de números racionais entre $\frac{1}{2}$ e $\frac{2}{3}$. Note que esta situação não acontecia nos inteiros: entre um número inteiro $a$ e seu consecutivo $a+1$, não é possível encontrar nenhum número inteiro. Por causa desta particularidade, dizemos que o conjunto dos números racionais é "denso" na reta, ou seja, entre dois números racionais existe uma infinidade de outros números racionais. Vamos generalizar:

Note que a idéia de "consecutivo" não se aplica a números racionais.

**Proposição 4.** Sejam $x$ e $y$ números racionais com $x < y$. Então existe um número racional $z$ tal que $x < z < y$.

**Demonstração.**

Sejam $z = \frac{1}{2}(x+y)$; $z < y$, pois:

$x < y$ (somando $y$ a ambos os membros da desigualdade)

$x + y < y + y$

$x + y < 2y$ (multiplicando ambos os membros por $\frac{1}{2}$)

$\frac{1}{2}(x + y) < y$

$z < y$.

Analogamente provamos que $x < z$.

■

## Exercícios propostos

34) J. J. Sylvester (1814 – 1897) propôs o seguinte método para escrever um número racional $x$, $0 < x < 1$, como soma das frações unitárias:

i) Achar a maior fração unitária que seja menor que a fração dada.

ii) Subtrair essa fração unitária da fração dada.

iii) Achar a maior fração unitária menor que a diferença obtida em ii.

iv) Subtrair desta diferença a fração unitária obtida em (iii).

v) Continuar o processo até que uma das diferenças seja uma fração unitária.

Aplicar este processo às frações treze vinte avos, quatro quinze avos, nove vinte e quatro avos e sete cinqüenta e dois avos.

35) Em um mapa, um centímetro representa dezesseis quilômetros. Qual a distância real representada por cinco centímetros e meio?

36) Ache duas frações ordinárias positivas, respectivamente iguais a um meio e quatro quintos, de maneira que a soma de seus termos (numerador e denominador) coincida e seja a menor possível.

37) Ache um número racional igual a $\frac{1001}{715}$ cuja soma do numerador com o denominador seja $48$.

38) Ache um número racional igual a $\frac{399}{1463}$ cuja diferença entre seu denominador e seu numerador seja $184$.

39) Ache dois números racionais de denominadores $5$ e $7$, cuja soma é igual a $\frac{26}{35}$.

40) Ache dois números racionais de denominadores $3$ e $11$, cuja diferença é igual a $\frac{6}{33}$.

41) Existem dois números racionais de denominadores $7$ e $11$, com numeradores positivos, cuja soma é $\frac{30}{77}$?

42) Determine $r \in \mathbb{Z}$ de modo que as seguintes frações representem um inteiro:

a) $\frac{10r}{2r-1}$ b) $\frac{33r}{3r-1}$.

43) Sendo $n$ um número inteiro, mostre que são irredutíveis as frações:

a) $\frac{n-1}{n-2}$, $n \neq 2$ b) $\frac{n-1}{2n-1}$

c) $\frac{2n+1}{2n(n+1)}$, $n \neq 0$, $n \neq -1$.

44) a) Seja $x$ um número racional tal que $0 < x < 1$. Mostre que existe $r \in \mathbb{N}^*$ para o qual tem-se $\frac{1}{r+1} \leq x < \frac{1}{r}$.

b) Ache $r$ conforme a parte (a) nos seguintes casos: $a = \frac{7}{22}$; $a = \frac{47}{60}$.

# 6.10 A representação decimal

Em sua obra "De Thiend" (O décimo) de 1585, Simon Stevin tinha por objetivo mostrar através da representação decimal "como efetuar, com facilidade nunca vista, todos os cálculos necessários entre os homens, por meio de inteiros sem frações".

Já sabemos que os números racionais em sua forma fracionária possuem algoritmos próprios para as operações. A vantagem da representação decimal (isto é, o uso de $0,5$ ao invés de $\frac{1}{2}$, por exemplo) é aproveitar os algoritmos das operações já conhecidas para números inteiros, com alguns cuidados especiais. Por exemplo, ao somar $\frac{1}{2}+\frac{3}{5}$ representamos $\frac{1}{2}$ por $0,5$ e $\frac{3}{5}$ por $0,6$ e "armamos a conta" como se fossem números inteiros, colocando vírgula em baixo de vírgula.

$$\begin{array}{r} 0,5 \\ +0,6 \\ \hline 1,1 \end{array}.$$

Um procedimento similar é feito para a multiplicação e a divisão. Para podermos usufruir plenamente dessas facilidades, precisamos saber como "transitar" entre as representações fracionária e decimal confortavelmente. Inicialmente vamos responder duas perguntas:

1) Como encontrar uma representação decimal de um número racional que está na forma fracionária?
2) Como encontrar uma forma fracionária de um número em representação decimal?

Respostas das perguntas:

Vamos exemplificar a situação com a fração $\frac{7}{25}$; aprendemos que para responder a primeira pergunta basta dividir $7$ por $25$ e "continuar a conta", "abaixando" zeros quando for preciso.

$$\begin{array}{rl} 70 & \big|\underline{25} \\ 200 & 0,28 \\ 00 & \end{array}$$

Mas em que se baseia este processo? A resposta está no Algoritmo da Divisão em $\mathbb{Z}$; a "continuação da conta" é a repetição do Algoritmo multiplicando o resto por $10$. Observe:

$$7 = 0 \times 25 + 7 .$$

Multiplicamos o resto $7$ por $10$ (pois nosso sistema é decimal) e novamente usamos o Algoritmo para $7\times10$ e $25$:

$$7\times10 = 2\times25 + 20\,. \qquad (1)$$

Mais uma vez multiplicamos o resto $20$ por $10$ e usamos o Algoritmo para $20\times10$ e $25$:

$$20\times10 = 8\times25\,. \qquad (2)$$

Paramos o processo, pois o resto é zero. As igualdades (1) e (2) nos darão a representação decimal. Observe o procedimento:

Por (2) temos que $20 = \dfrac{8\times25}{10}$.

Substituindo em (1) temos que $7\times10 = 2\times25 + \dfrac{8\times25}{10}$;

Multiplicando ambos os membros por $\dfrac{1}{10}$ obtemos:

$$7 = \frac{1}{10}\times2\times25 + \frac{1}{10}\times\frac{8\times25}{10};$$

Usando as propriedades das operações em $\mathbb{Q}$, temos

$$7 = 25\times\frac{2}{10} + 25\times\frac{8}{100}$$

$$7 = 25\times\left(\frac{2}{10} + \frac{8}{100}\right);$$

Multiplicando ambos os membros por $\dfrac{1}{25}$, temos

$$\frac{7}{25} = \frac{2}{10} + \frac{8}{100}\text{, ou}$$

$$\frac{7}{25} = \frac{2}{10} + \frac{8}{10^2}\,. \qquad (3)$$

A igualdade (3) expressa o número $\dfrac{7}{25}$ como uma soma de frações cujos denominadores são potências de $10$ (são chamadas frações decimais), a base de nosso sistema de numeração: sete vinte e cinco avos é igual a dois décimos mais oito centésimos. Note também que as frações do membro da direita possuem algarismos em seus nu-

meradores, e estes algarismos constituem os algarismos que "aparecem depois da vírgula" na conta inicial. Como a parte inteira é zero, temos que

$$\frac{7}{25} = 0 + \frac{2}{10} + \frac{8}{10^2}.$$

A representação para a expressão do membro da direita é $0,28$. Concluímos então que para expressar um número racional em sua forma decimal usamos uma versão do Algoritmo da Divisão em $\mathbb{Z}$ para o numerador como dividendo e o denominador como divisor; isto sempre será possível, pois o denominador é sempre não nulo (lembre-se da hipótese do Algoritmo da Divisão: o número que faz o papel de divisor deve ser não nulo). Se $b$ é um número negativo, usamos o processo para $|b|$; por exemplo, a representação decimal de $-\frac{7}{25}$ é $-0,28$.

Este processo nos mostra também como encontrar a representação fracionária de um número em representação decimal. Por exemplo, a representação fracionária de $4,375$ é :

$$4,375 = 4 + \frac{3}{10} + \frac{7}{10^2} + \frac{5}{10^3} = \frac{4\times10^3 + 3\times10^2 + 7\times10 + 5}{10^3} = \frac{4375}{10^3}.$$

Note que o numerador da fração após a segunda igualdade é a representação decimal do inteiro $4375$.

Experimente agora encontrar a representação decimal de $\frac{2}{3}$.

$$\begin{array}{r|l} 20 & 3 \\ \cline{2-2} 20 & 0,666... \\ 20 & \\ 2 & \end{array}$$

Observe que os restos se repetem, dando origem a uma seqüência de algarismos "6" após a vírgula. A conta "continua" indefinidamente, e este fato é representado pelas reticências. Neste caso, dizemos que a representação decimal é uma "dízima periódica"; o algarismo (ou algarismos) que se repete é chamado o "período", que em nosso caso é o $6$. Na prática não usamos esta representação: na maioria das vezes truncamos o número e "paramos" em duas ou três casas decimais. Lembre-se sempre que, quando se faz isso, estamos

trabalhando com outro número; substituir $0,666666...$ por $0,666$ é substituir o número $\frac{2}{3}$ pelo número $\frac{666}{10^3}=\frac{333}{500}$.

Na maioria das situações reais, esta substituição pode ser irrelevante, mas um pequeno erro sempre existe. Observe também que, quando não há resto zero, os valores dos restos devem começar a se repetir, uma vez que são limitados pelo divisor (lembre-se do Algoritmo da Divisão em $\mathbb{Z}: 0 \le r < |b|$). Não corremos o risco dos restos serem todos diferentes!

Agora, vamos responder a segunda pergunta: como encontrar a representação fracionária de um número expresso por uma dízima periódica? Vamos exemplificar com o número $0,55555...$

Usando o que já sabemos, podemos escrever:

$$0,55555... = \frac{5}{10}+\frac{5}{10^2}+\frac{5}{10^3}+\frac{5}{10^4}+...$$

A soma no membro à direita é infinita, ou seja, tem uma infinidade de parcelas. É possível encontrar um número como resultado desta soma? Sim, neste caso é sempre possível. A justificativa para este fato baseia-se na idéia de "limite", um conceito fundamental em matemática que você irá estudar na disciplina de Cálculo. Observe que as parcelas da soma vão diminuindo:

$$\frac{5}{10} > \frac{5}{10^2} > \frac{5}{10^3} > \frac{5}{10^4} > ...$$

Observe também que cada parcela é a anterior multiplicada por $\frac{1}{10}$. Podemos então pensar na seqüência das parcelas $\frac{5}{10}, \frac{5}{10^2}, \frac{5}{10^3}, \frac{5}{10^4}, ...$ como uma **progressão geométrica** (abrevia-se PG) infinita, decrescente, de razão $\frac{1}{10}<1$ e primeiro termo igual a $\frac{5}{10}$. Progressões desta natureza admitem uma soma de todos os seus termos; chamando o primeiro termo de $a_1$ e a razão de $q$, a soma é dada pela fórmula

$$S=\frac{a_1}{1-q}.$$

**Não esqueça:** esta soma só é possível para progressões geométricas infinitas e *decrescentes*, isto é, com *razão menor do que* 1.

No exemplo anterior temos:

$$0,5555... = \frac{5}{10} + \frac{5}{10^2} + \frac{5}{10^3} + \frac{5}{10^4} + ... = \frac{\frac{5}{10}}{1 - \frac{1}{10}} = \frac{\frac{5}{10}}{\frac{9}{10}} = \frac{5}{10} \times \frac{10}{9} = \frac{5}{9}.$$

Vamos fazer mais alguns exemplos, estudando casos em que o período não aparece imediatamente após a vírgula, ou quando o período tem mais de um algarismo.

**Exemplos**

16) $1,27777... = 1 + \frac{2}{10} + \frac{7}{10^2} + \frac{7}{10^3} + \frac{7}{10^4} + ... =$

$$= 1 + \frac{2}{10} + (\frac{7}{10^2} + \frac{7}{10^3} + \frac{7}{10^4} + ...).$$

A soma entre parênteses é a soma dos termos de uma PG infinita, decrescente, de razão $\frac{1}{10}$ e primeiro termo igual a $\frac{7}{10^2}$. Usando a fórmula $S = \frac{a_1}{1-q}$, obtemos:

$$1,27777... = 1 + \frac{2}{10} + \frac{7}{10^2} + \frac{7}{10^3} + \frac{7}{10^4} + ... = 1 + \frac{2}{10} + (\frac{7}{10^2} + \frac{7}{10^3} + \frac{7}{10^4} + ...) =$$

$$= 1 + \frac{2}{10} + \frac{\frac{7}{10^2}}{1 - \frac{1}{10}} = 1 + \frac{2}{10} + \frac{7}{10^2} \cdot \frac{10}{9} = 1 + \frac{2}{10} + \frac{7}{90} = \frac{90 + 2 \times 9 + 7}{90} = \frac{115}{90} = \frac{23}{18}$$

17) $0,121212... = \frac{1}{10} + \frac{2}{10^2} + \frac{1}{10^3} + \frac{2}{10^4} + ...$

O período neste caso é 12; note que se agruparmos dois em dois os termos do membro à direita, ficamos com:

$$0,121212... = \frac{1}{10} + \frac{2}{10^2} + \frac{1}{10^3} + \frac{2}{10^4} + ... = \left(\frac{1}{10} + \frac{2}{10^2}\right) + \left(\frac{1}{10^3} + \frac{2}{10^4}\right) + ...$$

Efetuando as adições dos parênteses, temos:

$$0,121212... = \frac{1}{10} + \frac{2}{10^2} + \frac{1}{10^3} + \frac{2}{10^4} + ... = \frac{12}{10^2} + \frac{12}{10^4} + \frac{12}{10^6} ...$$

Esta nova soma que aparece à direita é a soma dos termos de uma PG infinita, decrescente, com primeiro termo igual a $\frac{12}{10^2}$. E a razão? Para sabermos a razão, devemos verificar qual o número que, multiplicado por um termo, resulta no termo seguinte. Neste caso, temos que $\frac{12}{10^2} \times \frac{1}{10^2} = \frac{12}{10^4}$, o que significa que a razão é $\frac{1}{10^2}$. Usando a fórmula da soma da PG, $\left(\frac{12}{10^2}, \frac{12}{10^4}, \frac{12}{10^6}, ...\right)$ obtemos:

$$\frac{12}{10^2} + \frac{12}{10^4} + \frac{12}{10^6} ... = \frac{\frac{12}{10^2}}{1 - \frac{1}{10^2}} = \frac{12}{10^2} \times \frac{10^2}{99} = \frac{12}{99} = \frac{4}{33}.$$

18) $1,4232323 = 1 + \frac{4}{10} + \frac{2}{10^2} + \frac{3}{10^3} + \frac{2}{10^4} + \frac{3}{10^5} + ...$

Separando as duas primeiras parcelas da soma, agrupamos as outras parcelas duas a duas e ficamos com:

$$1,4232323 = 1 + \frac{4}{10} + \left(\frac{2}{10^2} + \frac{3}{10^3}\right) + \left(\frac{2}{10^4} + \frac{3}{10^5}\right) + ...$$

Procedendo como no exemplo anterior, podemos identificar uma PG efetuando a soma dos termos entre parênteses:

$$1,4232323 = 1 + \frac{4}{10} + \frac{23}{10^3} + \frac{23}{10^5} + \frac{23}{10^7} + ...$$

A PG tem primeiro termo igual a $\frac{23}{10^3}$ e razão igual a $\frac{1}{10^2}$; usando a fórmula, temos:

$$1,4232323 = 1 + \frac{4}{10} + \frac{23}{10^3} + \frac{23}{10^5} + \frac{23}{10^7} + ... = 1 + \frac{4}{10} + \frac{\frac{23}{10^3}}{1 - \frac{1}{10^2}} =$$

$$= 1 + \frac{4}{10} + \frac{23}{10^3} \times \frac{10^2}{99} = 1 + \frac{4}{10} + \frac{23}{990} = \frac{990 + 4 \times 99 + 23}{990} = \frac{1409}{990}.$$

19) $0,999... = \frac{9}{10} + \frac{9}{10^2} + \frac{9}{10^3} + \frac{9}{10^4} + \frac{9}{10^5} + ...$

Este caso é como no exemplo inicial: a soma é de uma PG infinita, decrescente, cujo primeiro termo é $\frac{9}{10}$ e a razão é $\frac{1}{10}$. Temos então:

$$0,999... = \frac{9}{10} + \frac{9}{10^2} + \frac{9}{10^3} + \frac{9}{10^4} + \frac{9}{10^5} + ... = \frac{\frac{9}{10}}{1 - \frac{1}{10}} = \frac{9}{10} \times \frac{10}{9} = 1.$$

Note que acabamos de descobrir uma nova representação para o número 1: uma representação decimal em dízima periódica. Isto nos sugere que também os outros números inteiros podem ter uma representação desta forma. De fato, todos os números racionais podem ser representados por dízimas periódicas. Veja mais exemplos e faça as contas se não estiver convencido!

20) $1,9999... = 2$

21) $2,9999... = 3$

22) $3,49999... = 3,5$

23) $7,379999... = 7,38$

## Exercícios propostos

45) Escreva a representação fracionária irredutível dos seguintes números racionais:

a) $0,0305$

b) $-34,796$

c) $5,4444$

d) $0,0001$

e) $1,20202020...$

f) $3,41898989...$

g) $-5,097777...$

h) $34,59999...$

46)Dê a representação decimal infinita:

a) $0,54$ b) $42,123$

c) $1,59$ d) $2,01$

47) Na divisão de $4,5$ por $2,345$, temos que "igualar as casas depois da vírgula" antes de começar a dividir, preenchendo as casas que faltam por zeros; depois "cortamos as vírgulas e dividimos como inteiros. Dê uma justificativa para este procedimento.

48) Na multiplicação de $8,97$ por $0,567$, o resultado terá cinco casas decimais. Explique por quê.

49) Mostre que:

a) $\frac{56}{100} = 0,56$ b) $\frac{456}{10} = 45,6$

c) $\frac{34}{10^5} = 0,00034$

O que você conclui?

## 6.10.1 Existência da representação decimal finita

Já vimos que todo número racional admite uma representação decimal infinita periódica, as chamadas dízimas periódicas, mas nem todo número racional admite uma representação decimal finita. Como saber, sem fazer a conta, que um número racional admite uma representação decimal finita? Observemos alguns exemplos:

24) Como você já deve ter notado (exercício 49), frações cujo denominador é uma potência de 10 admitem uma representação decimal finita; por exemplo,

$$\frac{9}{10} = 0,9; \quad \frac{234}{100} = 2,34; \quad \frac{12}{10^4} = 0,0012; \quad \frac{231}{10^5} = 0,00231; \quad \textit{etc.}$$

25) Observe atentamente as frações com representação decimal finita:

$$\frac{21}{16}=1,3125; \quad \frac{345}{4}=86,25; \quad \frac{1}{32}=0,03125; \quad \frac{4351}{64}=67,984375$$

O que têm elas em comum? Os denominadores são potências de $2$. Neste caso, haverá uma representação decimal finita, ou seja, se a fração apresentar uma potência de $2$ no denominador, existirá uma representação finita.

26) Agora observe as frações seguintes e suas representações decimais finitas:

$$\frac{59}{25}=2,36; \quad \frac{298}{125}=2,384; \quad \frac{1}{5}=0,2; \quad \frac{73}{625}=0,1168.$$

Podemos notar aqui que os denominadores são potências de $5$. Se a fração apresentar uma potência de $5$ em seu denominador, ela terá uma representação decimal finita.

Vamos reunir as nossas investigações em um teorema:

**Teorema.** Um número racional $\frac{a}{b}$ em sua forma irredutível admite uma representação decimal finita quando o denominador $b$ não apresentar outros fatores além de $2$ e $5$. A representação será somente infinita periódica quando o denominador $b$ apresentar pelo menos um fator primo diferente de $2$ e diferente de $5$.

**Observação 14.** Note que o teorema só pode ser usado para frações irredutíveis! Por exemplo, $\frac{91}{26}$ apresenta o fator $13$ no denominador $(26=2\times13)$ e, mesmo assim, possui uma representação decimal finita, pois a fração não é irredutível: $\frac{91}{26}=\frac{7}{2}$ e o denominador $2$ é uma potência de $2$. Logo, a fração admite uma representação decimal finita.

**Observação 15.** Falamos que a vantagem da representação decimal é usar os mesmos algoritmos das operações dos inteiros; no entanto, é preciso que fique claro que *isso é possível para representações decimais finitas*. Não sabemos como somar $0,8888...$ com $0,7777...$, por exemplo. Para efetuar esta soma, devemos usar a representação fracio-

nária dos números $0,8888... = \frac{8}{9}$ e $0,7777... = \frac{7}{9}$. Somando-os nesta nova representação obtemos $\frac{8}{9} + \frac{7}{9} = \frac{15}{9} = \frac{5}{3}$, cuja representação decimal é $1,666...$

## 6.11 Potências em $\mathbb{Q}$

A idéia de potência de um número que aprendemos em $\mathbb{Z}$ permanece a mesma no conjunto dos racionais, independente da representação utilizada. Mas a existência de inversos em $\mathbb{Q}$ nos permite definir potências de expoentes negativos. Veja alguns exemplos:

27) $\left(\frac{4}{3}\right)^2 = \frac{4}{3} \times \frac{4}{3} = \frac{4 \times 4}{3 \times 3} = \frac{4^2}{3^2}$.

28) $(0,56)^3 = 0,56 \times 0,56 \times 0,56 = 0,175616$.

29) $(1,2222...)^3 = \left(1 + \frac{2}{9}\right) \times \left(1 + \frac{2}{9}\right) \times \left(1 + \frac{2}{9}\right) = \frac{11}{9} \times \frac{11}{9} \times \frac{11}{9} = \frac{1331}{729}$.

(lembre-se da obs. 14: só sabemos operar em representação fracionária ou em representação decimal finita!).

30) $\left(\frac{5}{8}\right)^{-2} = \left[\left(\frac{5}{8}\right)^{-1}\right]^2 = \left(\frac{8}{5}\right)^2 = \frac{8^2}{5^2} = \frac{64}{25}$.

**Observação 16.** Note que no exemplo 30 (de potência negativa) usamos o inverso; um número elevado à potência $-2$ é igual ao inverso do número elevado à potência $2$.

**Definição.** Seja $n$ um número inteiro, $n \geq 0$ e $\frac{a}{b}$ um número racional não nulo. Então:

Se $n$ é um número inteiro positivo, então $-n$ é um número negativo.

i) $\left(\frac{a}{b}\right)^0 = 1$.

ii) $\left(\frac{a}{b}\right)^n = \frac{a^n}{b^n}$.

iii) $\left(\frac{a}{b}\right)^{-n} = \left[\left(\frac{a}{b}\right)^{-1}\right]^n = \left(\frac{b}{a}\right)^n = \frac{b^n}{a^n}$.

### 6.11.1 Propriedades das potências em $\mathbb{Q}$

As propriedades das potências em $\mathbb{Q}$ permanecem as mesmas que em $\mathbb{Z}$; entretanto, agora podemos usar potências inteiras:

**Proposição 5.** Dados os números racionais $x$ e $y$ e os números inteiros $n$ e $m$, tem-se:

a) $x^n.x^m = x^{n+m}$

b) $(x^n)^m = x^{n.m}$

c) $(x.y)^n = x^n.y^n$

d) $\dfrac{x^n}{x^m} = x^{n-m}$

**Demonstração.** a), b) e c) demonstram-se por indução, como em $\mathbb{Z}$ (capítulo 5). Demonstra-se d) usando b) e a definição de divisão.

## 6.12 Existência de números que não são racionais

O conjunto dos números racionais possui quase todas as propriedades que precisamos para resolver os problemas básicos de matemática. Mas existem situações em que o conjunto dos números racionais não é suficiente. Basta lembrar que, para calcular a medida da diagonal de um quadrado de lado 1 pelo Teorema de Pitágoras, temos:

$$d^2 = 1^2 + 1^2$$
$$d^2 = 2\,.$$

Note que não é possível encontrar um número racional cujo quadrado é $2$. De fato, suponhamos que seja possível encontrar um número racional $\dfrac{a}{b}$, em sua forma irredutível, cujo quadrado é $2$.

$$\left(\frac{a}{b}\right)^2 = 2\,.$$

Pela propriedade das potências, temos:

$$\frac{a^2}{b^2} = 2\,.$$

Multiplicando ambos os lados por $b^2$ obtemos

1) $a^2 = 2b^2$.

Como $a$ e $b$ são números inteiros, a igualdade nos informa que $2 \mid a^2$.

Mas $2$ é primo; neste caso, temos que $2$ também é divisor de $a$, ou seja, $a$ é um número par, da forma $a = 2k$. Substituindo em 1), obtemos

$$(2k)^2 = 2b^2$$
$$4k^2 = 2b^2.$$

Pela lei do cancelamento da multiplicação temos que:

$$2k^2 = b^2.$$

Neste caso, também teremos que $2 \mid b^2$ e como $2$ é primo, $2$ é divisor de $b$.

Mas isto é uma contradição, pois o número $\frac{a}{b}$ está em sua forma irredutível (ou seja, não admite fatores comuns) e $2$ não pode ser um fator de $a$ e também de $b$. Esta contradição teve origem em nossa suposição da existência de um número racional cujo quadrado é $2$. Logo, este fato não pode ocorrer, ou seja, não existe um número racional cujo quadrado é $2$. Em outras palavras, o número cujo quadrado é $2$ não é um número racional.

Isto nos mostra que existe um campo numérico mais amplo que o conjunto dos números racionais e você já o conhece: o conjunto dos números reais, que acrescenta ao conjunto dos números racionais os números irracionais, ou seja, aqueles números que não podem ser expressos como razão de inteiros. Este conjunto você irá estudar com detalhes na disciplina de Introdução ao Cálculo.

## Exercícios propostos

50) Verifique se os números racionais a seguir admitem uma representação decimal finita, sem efetuar a divisão:

a) $\frac{57}{6}$

b) $\frac{78}{26}$

c) $\frac{45}{256}$

51) Ao dividirmos dois números racionais em representação decimal finita, o quociente também apresentará representação decimal finita?

52) Mostre que não existe um número racional cujo quadrado é $5$ (sugestão: item 6.12 do texto). Em seguida, mostre que não existe um número racional cujo quadrado é um número primo $p$.