

# 50

IDEIAS DE

# MATEMÁTICA

QUE VOCÊ PRECISA CONHECER



TONY CRILLY

 Planeta

50  
IDEIAS DE  
MATEMÁTICA  
QUE VOCÊ PRECISA CONHECER

*Tradução*  
Helena Londres

Copyright © Tony Crilli, 2007

Copyright © Editora Planeta, 2017

Título original: 50 maths ideas you really need to know *Preparação:* Arlete Sousa

*Revisão técnica:* Marcelo Soares *Revisão:* Luiz Pereira *Diagramação:* Balão Editorial *Capa:*

Compañía

*Adaptação para eBook:* Hondana

CIP-BRASIL. CATALOGAÇÃO-NA-FONTE  
SINDICATO NACIONAL DOS EDITORES DE LIVROS, RJ

**C946c**

Crilli, Tony

50 ideias de matemática que você precisa conhecer / Tony Crilli;  
[tradução Helena Londres]. – 1. ed. – São Paulo: Planeta, 2017.

Tradução de: 50 maths ideas you really need to know ISBN 978-85-  
422-0886-3

1. Matemática - Obras populares. I. Londres, Helena. II. Título.

**16-38739**

CDD: 510

CDU: 51

**2017**

Todos os direitos desta edição reservados à EDITORA PLANETA DO BRASIL LTDA.

Rua Padre João Manuel, 100 – 21º andar Edifício Horsa II – Cerqueira César

01411-000 – São Paulo – SP  
[www.planetadelivros.com.br](http://www.planetadelivros.com.br)  
[atendimento@editoraplaneta.com.br](mailto:atendimento@editoraplaneta.com.br)

# Sumário

## Introdução

- 01 Zero
- 02 Sistemas numéricos
- 03 Frações
- 04 Quadrados e raízes quadradas
- 05  $\pi$
- 06 e
- 07 Infinito
- 08 Números imaginários
- 09 Primos
- 10 Números perfeitos
- 11 Números de Fibonacci
- 12 Retângulos áureos
- 13 Triângulo de Pascal
- 14 Álgebra
- 15 Algoritmo de Euclides
- 16 Lógica
- 17 Prova
- 18 Conjuntos
- 19 Cálculo
- 20 Construtos
- 21 Triângulos
- 22 Curvas
- 23 Topologia
- 24 Dimensão

- 25 Fractais**
- 26 Caos**
- 27 O postulado das paralelas**
- 28 Geometria discreta**
- 29 Grafos**
- 30 O problema das quatro cores**
- 31 Probabilidade**
- 32 Teoria de Bayes**
- 33 O problema do aniversário**
- 34 Distribuições**
- 35 A curva normal**
- 36 Conectando dados**
- 37 Genética**
- 38 Grupos**
- 39 Matrizes**
- 40 Códigos**
- 41 Contagem avançada**
- 42 Quadrados mágicos**
- 43 Quadrados latinos**
- 44 Matemática financeira**
- 45 O problema da dieta**
- 46 O caixeiro-viajante**
- 47 Teoria dos jogos**
- 48 Relatividade**
- 49 O último teorema de Fermat**
- 50 Hipótese de Riemann**

**Glossário**

**Índice**

# Introdução

A matemática é uma matéria vasta, impossível de ser conhecida por inteiro. O que se pode fazer é explorar e descobrir um caminho próprio. As possibilidades que são abertas aqui nos conduzem a outras eras, a culturas diferentes e a ideias que vêm intrigando os matemáticos há séculos.

A matemática é, ao mesmo tempo, antiga e moderna e foi construída a partir de influências amplamente difundidas, tanto culturais como políticas. Da Índia e da Arábia derivamos nosso sistema moderno de numeração, mas esse sistema é repleto de pegadinhas históricas. A “base 60” dos babilônios, de 2000 ou 3000 a.C., aparece em nossa própria cultura – temos 60 segundos em uma hora; um ângulo reto ainda tem  $90^\circ$  e não 100 graus, como a França revolucionária adotou em um primeiro movimento que buscava a decimalização.

Os triunfos tecnológicos da era moderna dependem da matemática, e certamente ninguém mais se vangloria de não ter sido bom nessa disciplina na escola. É claro que a matemática da escola é algo diferente, muitas vezes ensinada com foco nas avaliações. A escola sofre a pressão do tempo, o que também não ajuda, porque a matemática é uma matéria em que não há nenhum mérito em ser rápido, e as pessoas precisam de tempo para assimilar as ideias. Alguns dos maiores matemáticos foram bastante lentos em aprender os profundos conceitos do assunto.

Não há pressa com este livro. Ele pode se transformar até

mesmo em uma diversão. Vá com calma e descubra o que essas ideias, de que você pode ter ouvido falar, significam na verdade. Começando com o Zero, ou em qualquer outra parte, se quiser, você pode embarcar em uma viagem entre ilhas de ideias matemáticas. Por exemplo, é possível se tornar conhecedor da Teoria dos Jogos e em seguida ler sobre os Quadrados Mágicos. Ou, como alternativa, você pode passar de retângulos áureos para o famoso último teorema de Fermat, ou qualquer outro caminho.

Estamos em uma época instigante para a matemática, pois alguns de seus principais problemas foram resolvidos recentemente. Os modernos desenvolvimentos computacionais ajudaram com alguns deles, mas foram inúteis com outros. O Problema das Quatro Cores foi resolvido com a ajuda de um computador, mas a hipótese de Riemann permanece sem solução – por computador ou por qualquer outro meio.

A matemática é para todos. A popularidade do Sudoku é prova de que as pessoas podem praticar matemática (sem saber), e ainda por cima curtir-la. Na matemática, do mesmo modo que na arte ou na música, há gênios, mas a história deles não é a história toda. Você verá diversos pensadores entrando e saindo de alguns capítulos e reaparecendo em outros. Leonhard Euler, cujo tricentenário ocorreu em 2007, é um visitante frequente destas páginas. Mas o progresso real na matemática é obra de “muitos” e vem se acumulando ao longo dos séculos. A escolha de 50 temas é pessoal, mas tentei manter um equilíbrio. Há itens corriqueiros e itens avançados, matemática pura e aplicada, abstrata e concreta, a velha e a nova. Embora seja uma matéria



coesa, a dificuldade em escrever este livro não foi a escolha dos temas, mas quais deixar de fora. Poderiam ser 500 ideias, mas 50 bastam para um bom início em sua carreira matemática.

# 01 Zero

## linha do tempo

700 a.C.	628 d.C.	830	1100	1202
os babilônios usam o zero como variável em seu sistema numérico	Brahmagupta usa o zero e estabelece regras para seu uso com outros algarismos	Mahavira tem ideias sobre como o zero interage com outros algarismos	Bhaskara usa 0 como um símbolo na álgebra e tenta mostrar como manipulá-lo.	Fibonacci usa o símbolo extra 0 acrescentado ao sistema indo-arábico de algarismos 1, ..., 9, mas não como um número feito eles

**Ainda crianças, fazemos uma entrada um tanto instável no mundo dos números. Aprendemos que o 1 é o primeiro no “alfabeto dos números” e que ele introduz os números inteiros 1, 2, 3, 4, 5... Contar números é apenas isso: contam-se coisas reais – maçãs, laranjas, bananas, peras *etc.* Só mais tarde começamos a contar o número de maçãs em uma caixa quando não há maçã alguma.**

Até mesmo os gregos, que fizeram a ciência e a matemática progredirem em saltos quânticos, e os romanos, conhecidos por suas façanhas na engenharia, não tinham um modo eficaz de lidar com o número de maçãs em uma caixa vazia. Eles não conseguiram dar um nome ao “nada”. Os romanos tinham seus modos de combinar I, V, X, L, C, D e M, mas onde estava o 0? Eles não contavam o “nada”.

**Como o zero passou a ser aceito?** Imagina-se que o uso de um símbolo designando “o nada” teve origem há milhares de anos. A civilização maia, onde é hoje o México, usou o zero sob diversas formas. Um pouco mais tarde, o astrônomo Claudius Ptolomeu, influenciado pelos babilônios, usou um símbolo semelhante ao nosso 0 moderno como uma espécie de símbolo em seu sistema numérico. Como símbolo, o zero podia ser usado

para distinguir entre exemplos (na notação moderna), tal como 75 e 705, em vez de se basear no contexto, como fizeram os babilônios. Pode-se comparar isso com a introdução da “vírgula” à linguagem – tanto para ajudar na leitura como no significado correto. No entanto, exatamente como a vírgula, ele vem com um conjunto de regras para seu uso – tem de haver regras para o uso do zero.

Brahmagupta, matemático indiano do século VII, tratou o zero como um “número”, e não apenas como um símbolo, e estabeleceu regras para lidar com ele. Entre essas regras estavam “a soma de um número positivo e um zero é positiva” e “a soma de zero com zero é zero”. Ao pensar no zero como um número, em vez de um símbolo, ele estava bastante avançado. O sistema de numeração indo-arábico, que incluía o zero dessa maneira, foi difundido no Ocidente por Leonardo de Pisa – Fibonacci – em seu *Liber Abaci* (*O livro de contar*), publicado pela primeira vez em 1202. Criado no Norte da África e instruído na aritmética indo-arábica, ele reconheceu o poder do uso do sinal 0 a mais combinado aos símbolos hindus 1, 2, 3, 4, 5, 6, 7, 8 e 9.

O lançamento do zero no sistema numérico apresentou um problema que Brahmagupta tinha abordado brevemente: como deveria esse “intruso” ser tratado? Ele tinha dado o pontapé inicial, mas suas soluções eram vagas. Como poderia o zero ser integrado ao sistema de aritmética existente de um modo mais preciso? Alguns ajustes eram diretos. Quando se tratava de adição e multiplicação, o 0 se encaixava, mas as operações de subtração e divisão não se acomodavam bem com o “estranho”. Havia necessidade de significados para garantir que o 0 se

harmonizasse com o restante da aritmética aceita.

**Como funciona o zero?** A soma e a multiplicação com zero são diretas e evidentes – você pode adicionar 0 a 10 para obter 10 – mas queremos dizer “adicionar” em um modo menos imaginativo da operação numérica. Acrescentar 0 a um número não muda esse número, enquanto multiplicar 0 por qualquer número sempre resulta em zero. Por exemplo, temos  $7 + 0 = 7$  e  $7 \times 0 = 0$ . A subtração é uma operação simples, mas pode levar a negativos,  $7 - 0 = 7$  e  $0 - 7 = -7$ , enquanto a divisão envolvendo zero apresenta dificuldades. Imaginemos uma extensão a ser medida com uma régua. Suponhamos que a régua tem exatamente 7 unidades de comprimento. Estamos interessados em saber quantas réguas é possível estender ao longo de nossa extensão dada. Se a extensão a ser medida é exatamente 28 unidades, a resposta é 28 divididos por 7, ou em símbolos,  $28 \div 7 = 4$ . Uma notação melhor para expressar essa divisão é

$$\frac{28}{7} = 4$$

e depois fazer uma “multiplicação cruzada” para escrever isso em termos de multiplicação, como  $28 = 7 \times 4$ . E agora, o que pode ser feito com 0 dividido por 7? Para ajudar na sugestão de uma solução para esse caso, vamos considerar a resposta  $a$  de modo que

$$\frac{0}{7} = a$$

Isso equivale, pela multiplicação cruzada, a  $0 = 7$ . Se for esse o caso, o único valor possível para  $a$  é o próprio 0, porque se a multiplicação de dois números der 0, um deles tem de ser 0.

Evidentemente não é 7, então  $a$  tem de ser zero.

Essa não é a principal dificuldade com o 0. O perigo maior está na divisão *por* 0. Se tentarmos tratar  $7/0$  do mesmo modo como fizemos com  $0/7$ , teremos a equação

$$\frac{7}{0} = b$$

pela multiplicação cruzada,  $0 \times b = 7$  e acabamos com  $0 = 7$ , que é absurdo. Se admitirmos a possibilidade de  $7/0$  ser um número, passamos a ter o potencial para o caos numérico em grande escala. A saída para isso é dizer que  $7/0$  é indefinido. Não é possível tirar qualquer sentido da operação de dividir 7 (ou qualquer outro número) por 0, de modo que simplesmente não permitimos que essa equação aconteça. De maneira semelhante, não é permissível colocar uma vírgula no meio de uma palavra sem que isso seja considerado uma tolice.

O matemático indiano Bhaskara, do século XII, seguindo os passos de Brahmagupta, refletiu sobre a divisão por 0 e sugeriu que um número dividido por 0 era infinito. Isso é razoável porque se dividimos um número por outro muito pequeno, obtemos uma resposta muito grande. Por exemplo, 7 dividido por um décimo é 70, e por um centavo, é 700. Tornando o denominador cada vez menor, a solução vai ser cada vez maior. Na suprema minimidade, o 0 propriamente dito, a solução seria o infinito. Ao adotar essa forma de raciocínio, ficamos na posição de explicar um conceito ainda mais estranho – ou seja, o infinito. Lutar contra o infinito não ajuda; o infinito (com sua notação padrão  $\infty$ ) não obedece às regras comuns da aritmética e não é um número no senso comum.

Se  $7/0$  é um problema, o que pode ser feito com o ainda mais estranho  $0/0$ ? Se  $0/0 = c$ , pela multiplicação cruzada chegamos à equação  $0 = 0 \times c$  e ao fato de que  $0 = 0$ . Isso não é particularmente elucidativo, mas tampouco é absurdo. Na verdade,  $c$  pode ser qualquer número e não chegamos a uma impossibilidade. Chegamos à conclusão de que  $0/0$  pode ser qualquer coisa; nos círculos matemáticos de renome é chamado de “indeterminado”.

Para resumir, quando pensamos em dividir por zero chegamos à conclusão de que é melhor excluir a operação do modo como fazemos cálculos. A aritmética pode ser conduzida de maneira satisfatória sem isso.

**Para que serve o zero?** Simplesmente não conseguimos viver sem o 0. O progresso da ciência dependeu dele. Falamos sobre  $0^\circ$  de longitude,  $0^\circ$  na escala de temperatura e, do mesmo modo, energia zero e gravidade zero. O zero entrou para a linguagem não científica com ideias como zero-hora e tolerância-zero.

Pode-se, no entanto, fazer um uso ainda maior dele. Se você desce da calçada da 5ª Avenida em Nova York e entra no Empire State Building, você está no saguão de entrada, no Andar Número 1. Isso faz uso da capacidade dos números de ordenar, 1 como “primeiro”, 2 como “segundo”, e daí por diante, até 102 como “centésimo segundo”. Na Europa eles têm um Andar 0, mas relutam em chamá-lo assim.

## **Tudo a respeito de nada**

A soma de zero e um número positivo é positiva

A soma de zero e um número negativo é negativa

A soma de um positivo e um negativo é a sua diferença; ou, se forem iguais, zero

Zero dividido por um número positivo ou negativo ou é zero ou é expresso como uma fração com zero como numerador e a quantidade finita como denominador

## **Brahmagupta, a.D. 628**

A matemática não poderia funcionar sem zero. Ele está no núcleo dos conceitos matemáticos que fazem o sistema numérico, a álgebra e a geometria funcionarem. Na linha de número 0 está o número que separa os números positivos dos negativos e que, portanto, ocupa uma posição privilegiada. No sistema decimal, o zero serve como um símbolo que nos permite usar tanto números imensos como microscópicos.

Ao longo do curso de centenas de anos, o zero passou a ser aceito e utilizado, tornando-se uma das maiores invenções do homem. G.B. Halsted, matemático norte-americano do século XIX, adaptou o *Sonho de uma noite de verão* de Shakespeare escrevendo-o como a máquina de progresso que dá “ao aéreo nada, não apenas uma moradia local e um nome, uma imagem, um símbolo, mas poder útil, é a característica de onde brotou a

competição hindu”.

Quando o zero foi introduzido, devem tê-lo considerado estranho, mas os matemáticos têm o hábito de se ligarem a conceitos esquisitos que se provarão úteis muito mais tarde. O equivalente atual ocorre na teoria dos conjuntos, onde o conceito de um *conjunto* é uma coleção de elementos. Nessa teoria, o  $\emptyset$  designa um conjunto sem elementos, o assim chamado “conjunto vazio”. Agora é uma ideia estranha, mas do mesmo modo que o 0, é indispensável.

**A ideia condensada:  
nada é bem  
alguma coisa**



## 02 Sistemas numéricos

### linha do tempo

30000 a.C.	2000 a.C.	600 d.C.	1200	1600
povos paleolíticos na Europa traçam marcas de números em ossos	os babilônios usam símbolos que significam números	os primórdios de nossa notação decimal moderna são usados na Índia	o sistema indo-arábico de se escrever os algarismos 1, ..., 9 se espalha	os símbolos do sistema decimal tomam suas formas modernas reconhecíveis.

**Um sistema numérico é um método usado para lidar com o conceito de “quantos”. Culturas diferentes, em épocas diferentes, adotaram vários métodos, indo do básico “um, dois, três, muitos” à altamente sofisticada notação de posicionamento decimal que usamos hoje em dia.**

Os sumérios e babilônios, que há cerca de 4 mil anos habitavam a região que hoje é constituída por Síria, Jordânia e Iraque, usavam o sistema de valor posicional em sua prática diária. Chamamos isso de sistema de valor posicional porque você pode identificar o “número” pela posição de um símbolo. Além disso, eles usavam 60 como unidade básica – o que hoje chamamos sistema de “base 60”. Vestígios da base 60 ainda existem: 60 segundos em um minuto, 60 minutos por hora. Ao medir ângulos, ainda calculamos o ângulo total como sendo  $360^\circ$ , apesar da tentativa do sistema métrico de transformá-lo em 400 graus (de modo que cada ângulo reto seria igual a 100 graus).

Embora o principal interesse dos nossos ancestrais pelos números fosse para fins práticos, há algumas evidências de que essas culturas primitivas ficaram curiosas com a matemática propriamente dita e gastaram tempo das tarefas práticas da vida para explorá-la. Essas explorações incluíram o que podemos chamar de “álgebra” e também as propriedades das figuras

geométricas.

O sistema egípcio, a partir do século XIII a.C., passou a usar a base dez com um sistema de sinais hieroglíficos. Um feito notável dos egípcios foi desenvolverem um sistema para lidar com as frações, mas a atual notação decimal do valor posicional vem dos babilônios, mais tarde refinada pelos hindus. A vantagem dele é o modo como pode ser usado tanto para expressar números muito pequenos como muito grandes. Pelo uso apenas dos algarismos indo-arábicos 1, 2, 3, 4, 5, 6, 7, 8 e 9, os cálculos podem ser feitos com relativa facilidade. Para ver isso, vamos dar uma olhada no sistema romano. Ele se adequava às suas necessidades, mas apenas especialistas no sistema eram capazes de usá-lo para efetuar cálculos.

**O sistema romano** Os símbolos básicos usados pelos romanos eram os “dez” (I, X, C e M) e as “metades” desses (V, L e D). Os símbolos são combinados para formar outros. Foi sugerido que o uso de I, II, III e IIII deriva da aparência dos nossos dedos, V do formato da mão, e invertendo-o e juntando os dois para formar o X obtemos duas mãos ou dez dedos. C vem de *centum*, e M de *mille*, as palavras em latim para cem e mil, respectivamente. Os romanos usavam também o S para “um meio” e um sistema de frações com base em 12.

O sistema romano fazia algum uso de um método “antes e depois” para produzir os símbolos necessários, mas ao que parece esse sistema não foi adotado de modo uniforme. Os antigos romanos preferiam escrever IIII, e o IV só foi introduzido mais tarde. A combinação IX parece ter sido usada,

mas um romano teria querido dizer 9 1/2 se estivesse escrito *SIX* (SEIS [S=1/2, IX=9])! Esses são os números *básicos* do sistema romano, com alguns acréscimos vindos dos tempos medievais: Não é fácil lidar com algarismos romanos. Por exemplo, o significado de MMMCDXLIIII só se torna claro quando introduzimos parênteses mentais, de modo que (MMM)(CD)(XL)(IIII) é então lido como 3000 + 400 + 40 + 4 = 3444. Mas tente somar MMMCDXLIIII + CCCXCIIII. Um romano com noções de arte teria atalhos e truques, mas para nós é difícil obter a resposta certa sem primeiro calculá-la no sistema decimal e depois traduzi-la para a notação romana:

## Sistema numérico romano

### Império romano

S meio

I um

V cinco

X dez

L cinquenta

C cem

D quinhentos

M mil

### Apêndices medievais

$\overline{V}$  cinco mil

$\overline{X}$  dez mil

$\overline{L}$  cinquenta mil

$\overline{C}$  cem mil

$\overline{D}$  quinhentos mil

$\overline{M}$  um milhão

**Soma:**

**3.444**       $\rightarrow$       MMMCDXLIIII

+394       $\rightarrow$       CCCXCIIII  
 = 3.838       $\rightarrow$       MMMDCCCXXXVIII

A multiplicação de dois números é muito mais difícil e pode ser impossível dentro do sistema básico, até para os romanos! Para multiplicar  $3.444 \times 394$  precisamos dos apêndices medievais.

### Multiplicação

3444	->	MMMCDXLIII
x 394	->	CCCXCIII
=1.356.936	->	$\overline{M} \overline{C} \overline{C} \overline{C} \overline{L} \overline{V}$ IMCMXXXVI



Um relógio Luís XIII

Os romanos não tinham um símbolo específico para zero. Se você pedisse a um cidadão romano vegetariano que anotasse quantas garrafas de vinho tinha consumido naquele dia, ele podia escrever III, mas se você perguntasse quantas galinhas tinha comido, ele não podia escrever 0. Vestígios do sistema romano sobrevivem nas páginas de alguns livros (mas não neste) e em pedras fundamentais de edifícios. Algumas construções numéricas nunca foram usadas pelos romanos, como MCM para 1900. Elas foram introduzidas por motivos de estilo em épocas modernas. Os romanos teriam escrito MDCCCC. Luís, o décimo quarto rei da França, hoje universalmente conhecido como Luís XIV, na verdade preferia ser conhecido como Luís XIII e fez uma lei para que todos os seus relógios

mostrassem as 4h como IIII horas. **Números inteiros decimais**  
 Identificamos “números” com os números decimais. O sistema decimal tem base 10, usando os algarismos 0, 1, 2, 3, 4, 5, 6, 7, 8, e 9. Na verdade, esse sistema é baseado em “dezenas” e “unidades”, mas as unidades podem ser absorvidas na “base 10”. Quando escrevemos o número 394, podemos explicar seu significado decimal dizendo que ele é composto de 3 centenas, 9 dezenas e 4 unidades, e poderíamos escrever  $394 = 3 \times 100 + 9 \times 10 + 4 \times 1$

Isso pode ser escrito usando “potências” de 10, também conhecidas como “expoentes” ou “índices”,  $394 = 3 \times 10^2 + 9 \times 10^1 + 4 \times 10^0$

onde  $10^2 = 10 \times 10$ ,  $10^1 = 10 \times$  e por fora concordamos que  $10^0 = 1$ . Nesta expressão vemos mais claramente a base *decimal* do nosso sistema numérico do dia a dia, um sistema que torna a soma e a multiplicação razoavelmente transparentes. **A vírgula do decimal** Até aqui examinamos a representação de números inteiros. Será que o sistema decimal pode dar conta de partes de um número, como 572/1.000?

Isso significa

$$\frac{572}{1.000} = \frac{5}{10} + \frac{7}{100} + \frac{2}{1.000}$$

Podemos tratar as “recíprocas” de 10, 100, 1.000 como potências *negativas* de 10, de modo que  $\frac{572}{1.000} = 5 \times 10^{-1} + 7 \times 10^{-2} + 2 \times 10^{-3}$

e isso pode ser escrito como 0,572, onde a vírgula indica o início das potências negativas de 10. Se acrescentamos isso à expressão

decimal para 394, obtemos a expansão decimal para o número  $394^{572} / 1.000$ , que é simplesmente 394,572.

Para números muito grandes, a notação decimal pode ser muito longa, então reverteremos, nesse caso, à “notação científica”. Por exemplo, 1.356.936.892 pode ser escrito como  $1,356936892 \times 10^9$ , que muitas vezes aparece como “ $1,356936892 \times 10E9$ ” em calculadoras ou computadores. Aqui, a potência 9 indica que o número tem uma unidade a menos de algarismos, e a letra *E* quer dizer “exponencial”. Algumas vezes podemos querer usar números ainda maiores, por exemplo, se estivermos falando do número de átomos de hidrogênio no universo conhecido. Esse número foi estimado como sendo cerca de  $1,7 \times 10^{77}$ . Do mesmo modo,  $1,7 \times 10^{-77}$ , com uma potência negativa, é um número muito pequeno e isso também é facilmente tratado usando notação científica. Pensar nesses números com os símbolos romanos não dá nem para a saída. **Zeros e uns** Embora a base 10 seja o trivial diário, algumas aplicações exigem outras bases. O sistema binário, que usa a base 2, está por trás da potência do computador moderno. A beleza do binário é que qualquer número pode ser expresso usando-se apenas os símbolos 0 e 1. O reverso dessa economia é que as expressões numéricas podem ficar muito longas.

Potências de 2

decimal

20

1

21

2

22

4

23

8

24	16
25	32
26	64
27	128
28	256
29	512
210	

**1.024**

Como poderíamos expressar **394** na notação binária? Dessa vez estamos lidando com potências de 2, e depois de algum cálculo é possível apresentar a expressão inteira como sendo  **$394 = 1 \times 256 + 1 \times 128 + 0 \times 64 + 0 \times 32 + 0 \times 16 + 1 \times 8 + 0 \times 4 + 1 \times 2 + 0 \times 1$**

Desse modo, separando os zeros e uns, **394** em binário é **110001010**.

Como as expressões binárias podem ser muito longas, frequentemente em computação aparecem outras bases. Essas são o sistema octal (em base 8), e o sistema hexadecimal (base 16). No sistema octal só precisamos dos símbolos 0, 1, 2, 3, 4, 5, 6, 7, enquanto o hexadecimal usa 16 símbolos. Nesse sistema de base 16, em geral usamos 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F. Como o 10 corresponde à letra A, o número **394** é representado em hexadecimal como 18A. É tão fácil quanto o ABC, que, temos de lembrar, é na realidade 2.748 em decimal!!!

# **A ideia condensada: como escrever números**

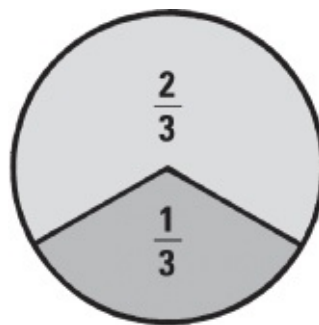


## 03 Frações

### linha do tempo

1800 a.C.	1650 a.C.	100 d.C.	1202	1585	1700
As frações são usadas nas culturas babilônicas	Os egípcios fazem uso de frações unitárias	Os chineses desenvolvem um sistema para o cálculo com frações	Leonardo de Pisa (Fibonacci) populariza a notação de barra para as frações	Simon Stevin estabelece uma teoria das frações decimais	A linha de fração “-” torna-se de uso geral (como em a/b)

**Uma fração é um “número fragmentado” – literalmente. Um modo apropriado para dividir um número inteiro é pelo uso de frações. Vamos tomar o exemplo tradicional, o famoso bolo, e parti-lo em três partes.**



A pessoa que ganha duas das três partes do bolo adquire uma fração equivalente a  $\frac{2}{3}$ . A pessoa sem sorte só ganha  $\frac{1}{3}$ . Unindo as duas porções do bolo, temos de volta o bolo inteiro, ou em frações,  $\frac{1}{3} + \frac{2}{3} = 1$ , onde 1 representa o bolo inteiro.

Aqui está outro exemplo. Você pode ter estado em uma liquidação e visto uma camisa anunciada como custando quatro quintos do preço original. Aqui a fração é escrita como  $\frac{4}{5}$ . Poderíamos dizer também que a camisa estava com um desconto de um quinto do preço original. Isso poderia ser escrito como  $\frac{1}{5}$  e vemos que  $\frac{1}{5} + \frac{4}{5} = 1$ , onde 1 representa o preço original.

Uma fração sempre tem a forma de um número inteiro “sobre” um número inteiro. O número de baixo é chamado de “denominador” porque nos diz quantas partes formam o todo. O número de cima é chamado de “numerador” porque nos diz quantas unidades da fração existem. Desse modo, uma fração na notação estabelecida sempre tem a aparência de

$$\frac{\text{numerador}}{\text{denominador}}$$

No caso do bolo, a fração que você poderá querer comer é  $\frac{2}{3}$ , onde o denominador é 3 e o numerador é 2. A fração  $\frac{2}{3}$  é constituída de duas frações unitárias de  $\frac{1}{3}$ .

Podemos também ter frações do tipo  $\frac{14}{5}$  (chamada fração imprópria), onde o numerador é maior do que o denominador. Ao dividirmos 14 por 5 obtemos 2 com um resto de 4 e a fração pode ser escrita como o número “misto”  $2\frac{4}{5}$ . Isso compreende o número 2 inteiro e a fração própria  $\frac{4}{5}$ . Alguns escritores primitivos escreviam isso como  $\frac{4}{5}2$ . As frações são geralmente representadas sob uma forma em que o numerador e o denominador (o “superior” e o “inferior”) não têm fatores comuns. Por exemplo, o numerador e o denominador de  $\frac{8}{10}$  têm um fator comum, o 2, porque  $8 = 2 \times 4$  e  $10 = 2 \times 5$ . Se escrevermos a fração  $\frac{8}{10} = \frac{4}{5}$  podemos “cortar” os 2 e então obter  $\frac{8}{10} = \frac{4}{5}$ , uma forma mais simples com o mesmo valor. Os matemáticos se referem às frações como “números racionais”, porque eles são razões entre dois números. Racionais eram os números que os gregos conseguiam “medir”.

**Soma e multiplicação** A coisa mais curiosa a respeito das frações

é que elas são mais fáceis de multiplicar do que somar. A multiplicação de números inteiros é tão complicada que tiveram de inventar métodos engenhosos para executá-la. Mas com as frações, é a soma que é mais difícil e toma algum tempo de raciocínio.

Vamos começar com a multiplicação de frações. Se você compra uma camisa a quatro quintos do preço original de £30, você acaba pagando o preço de liquidação de £24. Os £30 são divididos em cinco partes de £6 cada e quatro dessas cinco partes é  $4 \times 6 = 24$ , a quantia que você paga pela camisa.

Em seguida, o gerente da loja descobre que as camisas não estão vendendo assim tão bem, de modo que ele baixa ainda mais o preço, anunciando-as como  $1/2$  do preço de venda. Se for à loja, agora você consegue comprar a camisa por £12. Isso é  $1/2 \times 4/5 \times 30$ , que é igual a 12. Para multiplicar duas frações, basta multiplicar os denominadores e os numeradores:

$$\frac{1}{2} \times \frac{4}{5} = \frac{1 \times 4}{2 \times 5} = \frac{4}{10}$$

Se o gerente tivesse feito as duas reduções de uma só vez, ele teria anunciado as camisas como custando quatro décimos do preço original de £30. Isso é  $4/10 \times 30$ , que é £12.

A soma de duas frações é uma proposta diferente. A soma  $1/3 + 2/3$  não tem problema porque os denominadores são os mesmos. Simplesmente somamos os numeradores para obter  $3/3$ , ou 1. Mas como somamos dois terços de um bolo a quatro quintos de um bolo? Como podemos calcular  $2/3 + 4/5$ ? Se apenas pudéssemos dizer  $2/3 + 4/5 = 6/8$ , mas infelizmente não

podemos.

A soma de frações exige uma abordagem diferente. Para somar  $\frac{2}{3}$  a  $\frac{4}{5}$  é preciso primeiro expressar cada uma delas como frações com os *mesmos* denominadores. Primeiro, multiplicar a parte superior e a parte inferior de  $\frac{2}{3}$  por 5 para obter  $\frac{10}{15}$ . Agora a parte superior e a parte inferior de  $\frac{4}{5}$  são multiplicadas por 3 para obter  $\frac{12}{15}$ . Agora as duas frações têm 15 como denominador comum e para somá-las é só somar os numeradores:

$$\frac{2}{3} + \frac{4}{5} = \frac{10}{15} + \frac{12}{15} = \frac{22}{15}$$

**Conversão para decimais** No mundo da ciência e na maior parte das aplicações da matemática, os decimais são a forma preferida de se expressar frações. A fração  $\frac{4}{5}$  é a mesma coisa que a fração  $\frac{8}{10}$ , que tem 10 como denominador, então é possível escrever isso como o decimal 0,8.

As frações que têm 5 ou 10 como denominador são fáceis de converter. Mas como podemos converter, digamos,  $\frac{7}{8}$  sob a forma decimal? Basta saber que quando dividimos um número inteiro por outro, ou o resultado dá exato ou dá um determinado número de vezes com alguma coisa sobrando, que chamamos de “resto”.

Usando  $\frac{7}{8}$  como nosso exemplo, a receita para converter do modo fração para o decimal é a seguinte:

- Tente fazer o 8 caber dentro de 7. Não dá, ou você pode dizer que cabe 0 vezes com resto 7. Anotamos isso escrevendo zero seguido da vírgula decimal: “0,”.


- Agora vemos quantas vezes o 8 cabe em 70 (o resto do passo anterior multiplicado por 10). Dá 8 vezes, já que  $8 \times 8 = 64$ , então a resposta é 8 com o resto 6 ( $70 - 64$ ). Então escrevemos isso após primeiro passo, para obter “0,8”.
- Em seguida, vejamos quantas vezes 8 cabe em 60 (o resto do passo anterior vezes 10). Como  $7 \times 8 = 56$ , a resposta é 7 com 4 de resto. Anotamos isso e temos “0,87”.
- Distribua 8 em 40 (o resto do passo anterior multiplicado por 10). A resposta é exatamente 5, com 0 de resto. Quando obtemos resto 0, a receita está completa. Terminamos. A resposta final é “0,875”.


Se aplicarmos essa receita de conversão a outras frações, é possível que não terminemos jamais! Podemos continuar o processo sem parar; se tentarmos converter  $2/3$  em decimais, por exemplo, encontramos que em cada estágio o resultado de dividir 20 por 3 é 6, deixando 2 de resto. Então temos outra vez de ver quantos 6 cabem em 20, e nunca chegamos ao ponto em que o resto é zero. Nesse caso, temos o decimal infinito 0,666666... Isso é escrito como 0,6 com um ponto em cima ( $0,\dot{6}$ ) para indicar a “dízima periódica”.

Há diversas frações que continuam para sempre desse jeito. A fração  $5/7$  é interessante. Nesse caso, obtemos  $5/7 = 0,714285714285714285...$  e vemos que a sequência 714285 continua a se repetir. Se *qualquer* fração resulta em uma sequência que se repete, não conseguimos sequer anotá-la numa notação decimal que termine e a notação “pontuada” ganha vida própria. No caso de  $5/7$ , escrevemos  $5/7 = 0,714285$  com


pontinhos sobre cada algarismo (0,714285).

$$\frac{1}{2}$$


$$\frac{1}{3}$$


$$\frac{2}{3}$$


$$\frac{1}{4}$$


$$\frac{3}{4}$$


Frações egípcias

**Frações egípcias** Os egípcios do segundo milênio a.C. baseavam seu sistema de frações em hieróglifos que designavam frações *unitárias* – as frações cujo numerador é 1. Sabemos disso a partir do Papiro de Rhind, que está guardado no Museu Britânico. Era um sistema de frações tão complicado que só aqueles treinados em seu uso conheciam seus segredos íntimos e conseguiam fazer os cálculos corretos.

Os egípcios usavam algumas frações privilegiadas, como  $\frac{2}{3}$ , mas todas as outras frações eram expressas em termos de frações unitárias como  $\frac{1}{2}$ ,  $\frac{1}{3}$ ,  $\frac{1}{11}$  ou  $\frac{1}{168}$ . Essas eram suas frações “básicas”, a partir das quais todas as demais frações

podiam ser expressas. Por exemplo,  $5/7$  não é uma fração unitária, mas pode ser escrita em termos de frações unitárias

$$\frac{5}{7} = \frac{1}{3} + \frac{1}{4} + \frac{1}{8} + \frac{1}{168}$$

em que frações unitárias *diferentes* podem ser usadas. Uma característica do sistema é que pode haver mais de um modo de se escrever uma fração, e alguns modos são mais curtos do que outros. Por exemplo:

$$\frac{5}{7} = \frac{1}{2} + \frac{1}{7} + \frac{1}{14}$$

A “expansão egípcia” pode ter uso prático limitado, mas o sistema inspirou gerações de matemáticos puros e forneceu muitos problemas desafiadores, alguns dos quais permanecem sem solução até hoje. Por exemplo, uma análise completa dos métodos para se encontrar a *mais curta* expansão egípcia ainda aguarda um intrépido explorador matemático.

**A ideia condensada:  
um número  
sobre outro**

# 04 Quadrados e raízes quadradas

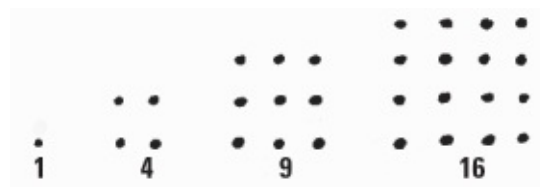
## linha do tempo

1750 a.C.	525 a.C.	c. 300 a.C.	630 d.C.	1550	1872
Os babilônios compilam tabelas de raízes quadradas	Os pitagóricos estudam números quadrados arrumados geometricamente	A teoria dos números irracionais de Eudoxo é publicada no Livro 5 dos <i>Elementos</i> de Euclides	Brahmagupta fornece métodos para o cálculo de raízes quadradas	É introduzido o símbolo para raízes quadradas	Richard Dedekind estabelece uma teoria dos números irracionais.

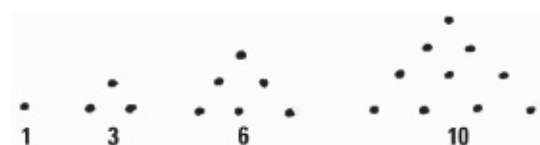
Se você gosta de desenhar quadrados com pontos, seus padrões de raciocínio são parecidos com os dos pitagóricos. Essa atividade era valorizada pela fraternidade que seguia seu líder, Pitágoras, um homem lembrado principalmente por “aquele teorema”. Ele nasceu na ilha grega de Samos, e sua sociedade religiosa secreta floresceu no sul da Itália. Os pitagóricos acreditavam que a matemática era a chave para a natureza do universo.

Ao contar os pontos, vemos que o primeiro “quadrado” à esquerda é feito com um ponto. Para os pitagóricos, o 1 era o número mais importante, imbuído de existência espiritual. Então começamos bem. A contagem dos pontos dos quadrados subsequentes nos dá números “quadrados”, 1, 4, 9, 16, 25, 36, 49, 64... Esses números são chamados de “quadrados perfeitos”. Você pode computar um número quadrado acrescentando pontos no formato fora do quadrado anterior, por exemplo  $9 + 7 = 16$ . Os pitagóricos não paravam nos quadrados. Eles tomavam em consideração outros formatos, como triângulos, pentágonos (a figura de cinco lados) e outros formatos poligonais (com muitos lados).





Os números triangulares se parecem com uma pilha de pedras. A contagem desses pontos nos dá 1, 3, 6, 10, 15, 21, 28, 36... Se quiser computar um número triangular, você pode usar o anterior e acrescentar o número de pontos na última fileira. Qual é o número triangular que vem depois de 10, por exemplo? Ele terá 5 pontos na última fileira, de modo que apenas somamos  $10 + 5 = 15$ .



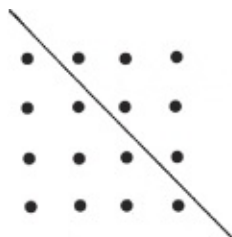
Se comparar os números quadrados e triangulares, você verá que o número 36 aparece nas duas listas. Mas há ainda uma ligação mais impressionante. Se tomar números triangulares *sucessivos* e somá-los, o que você obtém? Vamos experimentar e botar os resultados em uma tabela.

Soma de dois números triangulares sucessivos

1 + 3	<b>4</b>
3 + 6	<b>9</b>
6 + 10	<b>16</b>

	<b>25</b>
10 + 15	<b>25</b>
15 + 21	<b>36</b>
21 + 28	<b>49</b>
28 + 36	<b>64</b>

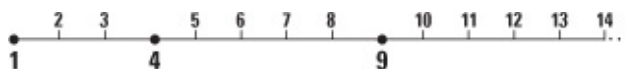
Exatamente! Ao somar dois números triangulares sucessivos, você obtém um número quadrado. É possível também ver essa “prova sem palavras”. Pense em um quadrado feito por 4 fileiras de pontos com uma linha diagonal traçada através dele. Os pontos acima da linha (no desenho) formam um número triangular e abaixo da linha está o número triangular seguinte. Essa observação se sustenta para quadrados de qualquer tamanho. É um atalho daqueles “diagramas de pontos” para medir áreas. A área de um quadrado cujo lado é 4 é  $4 \times 4 = 4^2 = 16$  unidades quadradas. Em geral, se o lado for chamado de  $x$ , então a área será  $x^2$ .

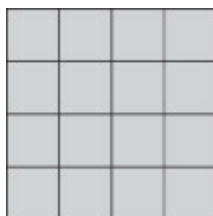


O quadrado  $x^2$  é a base do formato da parábola. Esse é o formato encontrado nas antenas parabólicas de satélites ou nos espelhos refletores dos faróis de carro. Uma parábola tem um ponto focal. Em uma antena, um sensor colocado no foco recebe os sinais refletidos quando as ondas paralelas vindas do espaço atingem a antena encurvada e se desviam na direção do ponto focal.

No farol de um carro, uma lâmpada posta no foco *envia* um feixe de luz paralelo. No esporte, arremessadores de peso, lançadores de dardos e arremessadores de martelo vão todos reconhecer a parábola como sendo o formato do trajeto em curva seguido por cada objeto ao cair.

**Raízes quadradas** Se nós invertermos a questão e quisermos encontrar o comprimento de um quadrado que tem uma dada área 16, a resposta é simplesmente 4. A raiz quadrada de 16 é 4 e é escrita como  $\sqrt{16} = 4$ . O símbolo para raiz quadrada é empregado desde os anos 1500. Todos os números quadrados têm belos números inteiros como raízes quadradas. Por exemplo,  $\sqrt{1} = 1$ ,  $\sqrt{4} = 2$ ,  $\sqrt{9} = 3$ ,  $\sqrt{25} = 5$ , e daí por diante. Há, no entanto, diversas falhas ao longo da linha de números entre esses quadrados perfeitos. Essas falhas são 2, 3, 5, 6, 7, 8, 10, 11...





Existe uma brilhante notação alternativa para as raízes quadradas. Do mesmo modo que  $x^2$  denota um número quadrado, pode-se escrever a raiz quadrada de um número como  $x^{1/2}$ , que se enquadra no dispositivo de se multiplicar números somando suas potências. Essa é a base para os logaritmos, inventados depois de ficarmos sabendo, por volta de 1600, que um problema de multiplicação de 18 quadrados e raízes quadradas poderia ser trocado por um problema de soma. Mas isso é outra história. Todos esses números têm raízes quadradas, mas essas raízes não são iguais a números inteiros. Praticamente todas as calculadoras têm uma tecla  $\sqrt{\phantom{x}}$  e usando-a encontramos, por exemplo, que  $\sqrt{7} = 2,645751311$ .

Vamos dar uma olhada na  $\sqrt{2}$ . O número 2 tem um significado especial para os pitagóricos porque é o primeiro número par (os gregos consideravam os números pares femininos e os ímpares, masculinos – e os números pequenos tinham personalidades distintas). Se você usar sua calculadora, vai obter 1,41421362, supondo que sua calculadora forneça tantas casas decimais. Essa é a raiz quadrada de 2? Para verificar, calcule  $1,41421362 \times 1,41421362$ . O resultado é 1,999999999. Isso não é bem 2, porque 1,41421362 é apenas uma aproximação da raiz quadrada de 2.

O que talvez seja notável é que o máximo que vamos obter é uma aproximação! A expansão decimal de  $\sqrt{2}$  a milhões de casas

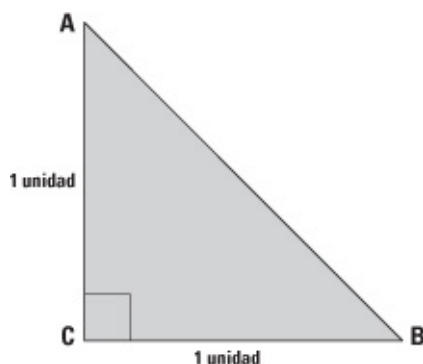
decimais nunca deixará de ser apenas uma aproximação. O número  $\sqrt{2}$  é importante na matemática, talvez não tão ilustre quanto  $\pi$  ou  $e$  (ver páginas 26–33), mas bastante importante para receber seu próprio nome – algumas vezes é chamado de “número pitagórico”.

**As raízes quadradas são frações?** A pergunta sobre se raízes quadradas são frações está ligada à teoria da medição conforme conhecida pelos gregos antigos. Imaginemos uma linha AB, cujo comprimento desejamos medir, e uma “unidade” invisível CD, com a qual queiramos medi-la. Para fazer a medição, colocamos a unidade CD sequencialmente contra AB. Se encaixarmos a unidade  $m$  vezes e a ponta da última unidade se encaixar perfeitamente com a extremidade de AB (no último ponto B), então o comprimento de AB será simplesmente  $m$ . Caso contrário, podemos colocar uma cópia de AB ao lado da original e continuar a medida com a unidade (ver figura). Os gregos acreditavam que em algum ponto, usando  $n$  cópias de AB e unidades  $m$ , a unidade iria se encaixar perfeitamente na extremidade final do  $m$  “ésimo” AB. O comprimento de AB seria então  $m/n$ . Por exemplo, se 3 cópias de AB forem alinhadas lado a lado e se 29 unidades se ajustassem ao longo, o comprimento de AB seria  $29/3$ .



Os gregos, além disso, pensaram em como calcular o comprimento do lado AB (a hipotenusa) de um triângulo em que um dos outros lados tem uma “unidade” de comprimento. Pelo

teorema de Pitágoras, o comprimento de AB poderia ser escrito simbolicamente como  $\sqrt{2}$  de modo que a questão é se  $\sqrt{2} = m/n$ .



Pela nossa calculadora, já vimos que a expressão decimal para  $\sqrt{2}$  é potencialmente infinita, e esse fato (de que não há fim para a expressão decimal) talvez indique que  $\sqrt{2}$  não é uma fração. Mas não há fim para o decimal 0,333333... e isso representa a fração  $1/3$ . Precisamos de argumentos mais convincentes.

**$\sqrt{2}$  é uma fração?** Isso nos traz uma das mais famosas provas na matemática. Ela segue a linha do tipo de prova que os gregos adoravam: o método de *redução ao absurdo* (*reductio ad absurdum*). Em primeiro lugar, eles supunham que  $\sqrt{2}$  não podia ser uma fração e uma “não fração” ao mesmo tempo. Essa é a lei da lógica chamada de “terceiro excluído”. Não existe um termo intermediário nessa lógica. Então, o que os gregos fizeram foi engenhoso. Eles supuseram que era uma fração e, aplicando a lógica rigorosa a cada passo, derivaram uma contradição, um “absurdo”. Então vamos lá. Suponhamos

$$\sqrt{2} = \frac{m}{n}$$

Pode-se supor também um pouquinho mais. É possível considerar que  $m$  e  $n$  não têm fatores comuns. Tudo bem, porque

se tivessem fatores comuns eles poderiam ser cortados antes de começarmos. (Por exemplo, a fração  $21/35$  é equivalente a  $3/5$  fatorado, depois de ter o fator comum 7 cortado).

Podemos elevar ao quadrado os dois lados da equação  $\sqrt{2} = m/n$  para obter  $2 = m^2/n^2$  e, desse modo,  $m^2 = 2n^2$ . É aqui que fazemos nossa primeira observação: já que  $m^2$  é 2 vezes alguma coisa, essa coisa tem de ser um número par. Em seguida, o próprio  $m$  não pode ser ímpar (porque a raiz quadrada de um número ímpar é ímpar), então  $m$  também é um número par.

Até aí a lógica é impecável. Como  $m$  é par, deve ser duas vezes alguma coisa, que podemos escrever como  $m = 2k$ . Elevando os dois lados ao quadrado, vamos ter  $m^2 = 4k^2$ . Combinando isso com o fato de que  $m^2 = 2n^2$  significa que  $2n^2 = 4k^2$  e cortando os 2 concluímos que  $n^2$  é par e o próprio  $n$  é par. Deduzimos assim, pela lógica mais rigorosa, que tanto  $m$  quanto  $n$  são pares e, portanto, têm um fator 2 em comum. Isso é contrário à nossa suposição de que  $m$  e  $n$  não têm fatores comuns. A conclusão, portanto, é que  $\sqrt{2}$  não pode ser uma fração.

Pode-se também provar que a sequência inteira de números  $\sqrt{n}$  (exceto quando  $n$  é um quadrado perfeito) não pode ser constituída de frações. Números que não podem ser expressos como frações são chamados “números irracionais”, de modo que observamos que há um número infinito de números irracionais.

**A ideia condensada.**

**A ideia consolidada.  
o caminho para os  
números irracionais**



## 05 $\pi$

### linha do tempo

2000 a.C.	250 a.C.	1706 d.C.	1761	1862
Os babilônios observam que $\pi$ é aproximadamente 3	Arquimedes dá a melhor aproximação de $\pi$ como 22/7	William Jones introduz o símbolo $\pi$	Lambert prova que o $\pi$ é irracional	Lindemann prova que o $\pi$ é transcendental

**$\pi$  é o número mais famoso na matemática. Esqueça todas as demais constantes da natureza, o  $\pi$  sempre estará no topo da lista. Se houvesse um Oscar para números, ele ganharia o prêmio todos os anos.**

$\pi$ , ou pi, é o comprimento do contorno de um círculo (a circunferência), dividido pelo comprimento da reta que atravessa seu centro (o diâmetro). Seu valor, a razão entre esses dois comprimentos, não depende do tamanho do círculo. Seja o círculo grande ou pequeno,  $\pi$  é realmente uma constante matemática. O círculo é o habitat natural do  $\pi$ , mas ocorre por toda parte na matemática, em locais nem remotamente ligados com o círculo.

**Arquimedes de Siracusa** A razão da circunferência para o diâmetro de um círculo é um assunto de interesse antigo. Por volta do ano 2000 a.C., os babilônios observaram que a circunferência tinha aproximadamente 3 vezes o tamanho do diâmetro.

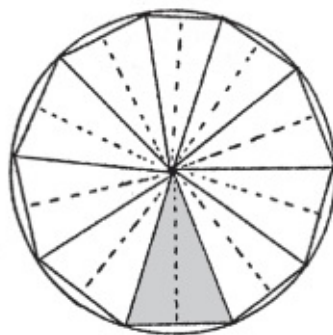
**Para um círculo de diâmetro  $d$  e raio  $r$ :**

circunferência =  $\pi d = 2\pi r$  área =  $\pi r^2$

**Para uma esfera de diâmetro  $d$  e raio  $r$ :**

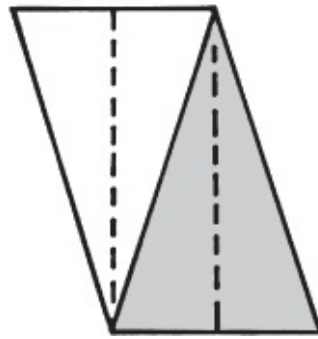
área da superfície =  $\pi d^2 = 4\pi r^2$  volume =  $\frac{4}{3} \pi r^3$

Foi Arquimedes de Siracusa quem de fato deu a partida na teoria matemática do  $\pi$ , por volta de 250 a.C. Arquimedes está lá no topo, entre os grandes. Os matemáticos adoram classificar seus colegas, e o põem no mesmo nível de Carl Friedrich Gauss (o “príncipe dos matemáticos”) e sir Isaac Newton. Sejam lá quais forem os méritos desse julgamento, fica claro que Arquimedes estaria em qualquer hall da fama matemático. Mas ele estava longe de se colocar numa torre de marfim – além de suas contribuições à astronomia, matemática e física, ele também projetou armas de guerra, como catapultas, alavancas e os “espelhos ardentes”, usados para manter os romanos afastados. De toda maneira, ele realmente tinha alguns aspectos de professor distraído; que outra coisa o induziria a pular de seu banho e correr pelado na rua gritando “Eureka” ao descobrir a lei do empuxo na hidrostática? Não há registros de como ele comemorou seu trabalho sobre  $\pi$ .



Dado que  $\pi$  é definido como a razão da circunferência de um círculo para seu diâmetro, o que ele tem a ver com a área do círculo? A determinação de que a área de um círculo de raio  $r$  é  $\pi r^2$  foi feita por *dedução*, embora provavelmente isso seja mais

conhecido do que a definição de  $\pi$  como sendo circunferência/diâmetro. O fato de que  $\pi$  funciona tanto para a área quanto para a circunferência é notável.



Como se pode mostrar isso? O círculo pode ser dividido em vários triângulos estreitos iguais com base de comprimento  $b$ , cuja altura é aproximadamente o raio  $r$ . Esses triângulos formam um polígono dentro do círculo, com área aproximada igual à do círculo. Tomemos 1.000 triângulos, para começar. O processo inteiro é um exercício de aproximação. Podemos unir cada par de triângulos adjacentes para formar um retângulo (aproximadamente) com área igual a  $b \times r$ , e com isso a área total do polígono será  $500 \times b \times r$ . Como  $500 \times b$  é cerca de metade da circunferência, ele tem como comprimento  $\pi r$  e a área do polígono será  $\pi r \times r = \pi r^2$ . Quanto mais triângulos tomarmos, maior será a aproximação, e no limite concluímos que a área do círculo é  $\pi r^2$ .

Arquimedes estimou o valor de  $\pi$  como limitado entre  $223/71$  e  $220/70$ . Então é a Arquimedes que devemos a conhecida aproximação  $22/7$  para o valor de  $\pi$ . A honra de designar o atual símbolo  $\pi$  se deve ao pouco conhecido William Jones, um matemático galês que se tornou vice-presidente da Royal Society

de Londres no século XVIII. Foi o matemático e físico Leonhard Euler quem popularizou o  $\pi$  no contexto da razão do círculo.

**O valor exato de  $\pi$**  Jamais saberemos o valor exato de  $\pi$  porque ele é um número irracional, fato provado por Johann Lambert em 1768. Sua expansão decimal é infinita, sem qualquer padrão previsível. As primeiras 20 casas decimais são 3,14159265358979323846... O valor da  $\sqrt{10}$  usado pelos matemáticos chineses é 3,166227766016837933199, e foi adotado por volta do ano 500 d.C. por Brahmagupta. Esse valor é de fato um pouco melhor do que o valor bruto de 3 e difere do valor de  $\pi$  na décima segunda casa decimal.

$\pi$  pode ser computado por uma *série* de números. Como bem se sabe, uma delas é

$$\frac{\pi}{4} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \frac{1}{11} + \dots$$

embora isso tenha uma convergência bastante lenta para  $\pi$  e quase impossível de calcular. Euler encontrou uma série notável que converge para  $\pi$ :

$$\frac{\pi^2}{6} = 1 + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \frac{1}{5^2} + \frac{1}{6^2} + \dots$$

O gênio autodidata Srinivasa Ramanujan concebeu algumas fórmulas de aproximação espetaculares para  $\pi$ . Uma delas, envolvendo apenas a raiz quadrada de 2 é:

$$\frac{9801}{4412} \sqrt{2} = 3.1415927300133056603139961890$$

Os matemáticos são fascinados pelo  $\pi$ . Embora Lambert tenha

provado que  $\pi$  não poderia ser uma fração, em 1882 o matemático alemão Ferdinand von Lindemann solucionou o problema mais importante associado a  $\pi$ . Ele mostrou que  $\pi$  é “transcendental”; ou seja,  $\pi$  não pode ser a solução de uma equação algébrica (uma equação que envolva apenas potências de  $x$ ). Ao solucionar o “enigma das eras”, Lindeman concluiu o problema da “quadratura do círculo”. Dado um círculo, o desafio era construir um quadrado de mesma área usando apenas um par de compassos e uma borda reta. Lindemann provou conclusivamente que isso não pode ser feito. Hoje em dia a expressão *quadratura do círculo* é o equivalente a uma impossibilidade.

O cálculo atual de  $\pi$  continuou em ritmo rápido. Em 1853, William Shanks alegou ter chegado a um valor correto até 607 casas (na verdade, estava correto apenas até 527). Nos tempos modernos, a busca do cálculo de  $\pi$  até cada vez mais casas decimais ganhou impulso através do computador. Em 1949,  $\pi$  foi calculado até 2.037 casas decimais, o que levou 70 horas em um computador ENIAC. Em 2002, o  $\pi$  tinha sido calculado a estonteantes 1.241.100.000.000 casas, mas ainda se trata de uma cauda que não para de crescer. Se ficássemos em pé no Equador e começássemos a escrever a dízima de  $\pi$ , pelos cálculos de Shank ela mediria 14 metros, mas o comprimento da expansão de 2002 daria cerca de 62 voltas em torno do mundo!

Diversas questões a respeito de  $\pi$  têm sido perguntadas e respondidas. Serão os algarismos de  $\pi$  aleatórios? Será possível encontrar uma sequência predeterminada na expansão? Nos anos 1950 isso parecia impossível de se saber. Ninguém

encontrou essa sequência nos 2.000 algarismos conhecidos de  $\pi$ . L.E.J. Brouwer, um grande matemático holandês, disse que a questão não tinha sentido, já que ele não acreditava que pudesse ser alcançada. De fato, esses algarismos foram encontrados em 1997 começando na posição 17.387.594.880, ou, usando a metáfora do Equador, cerca de 3 mil milhas antes de uma volta ter sido completada. Você encontrará dez “6” seguidos antes de ter completado 600 milhas, mas terá de esperar até que uma volta tenha sido completada e continuar por mais 3.600 milhas para encontrar dez “7” seguidos.

## $\pi$ na poesia

Se você quiser realmente lembrar dos primeiros valores na expansão de  $\pi$  talvez um pouco de poesia ajude. Seguindo a tradição inglesa de ensinar matemática no “jeito mnemônico” há uma variação brilhante do poema de Edgar Allen Poe, “O corvo”, feita por Michael Keith.

O poema original de Poe começa assim:

*The raven* – E.A. Poe

*Once upon a midnight dreary, while I pondered weak and weary,  
Over many a quaint and curious Volume of forgotten lore,<sup>[1]</sup>*

Variante de Keith para  $\pi$  começa assim:

Poe, E. – Near a Raven

*Midnights so dreary, tired and weary.  
Silently pondering volumes extolling all by now obsolete lore.*

A contagem das letras de cada palavra sucessiva na versão de Keith dá os primeiros 740 algarismos de  $\pi$ .

---

**A importância de  $\pi$**  Para que serve saber o  $\pi$  com tantas casas decimais? Afinal de contas, a maior parte dos cálculos só exige algumas casas decimais; provavelmente não mais do que dez casas são necessárias para qualquer aplicação prática, e a aproximação de Arquimedes de  $22/7$  é boa o bastante para a maior parte delas, mas os cálculos extensos não são apenas para diversão. São usados para testar os limites de computadores, além de exercerem um fascínio sobre o grupo de matemáticos que se denominou “os amigos do pi”.

Talvez o episódio mais estranho na história de  $\pi$  seja o projeto de lei do Estado de Indiana, nos EUA, de aprovar uma lei que fixava seu valor. Isso aconteceu no final do século XIX, quando um médico, dr. E.J. Goodwin, introduziu a lei para tornar o  $\pi$  “digerível”. Um problema prático encontrado nesse artigo de legislação foi a incapacidade do proponente em fixar o valor que ele queria. Para sorte de Indiana, a maluquice de legislar sobre  $\pi$  foi percebida antes de a lei ser sancionada. Desde então, os políticos deixaram o  $\pi$  em paz.

**A ideia condensada:  
quando o  $\pi$  foi aberto**

## 06 *e*

### linha do tempo

1618	1727	1748	1873	2007
John Napier encontra uma constante, $e$ , em conexão com os logaritmos.	Euler usa a notação $e$ em conexão com a teoria dos logaritmos; às vezes é chamado o número de Euler	Euler calcula $e$ até 23 casas decimais; é dado a ele o crédito da descoberta da famosa fórmula $e^{i\pi} + 1 = 0$ por volta dessa época.	Hermite prova que $e$ é um número transcendental.	$e$ é calculado na ordem de $10^{11}$ dígitos.

**O  $e$  é o garoto novato do bairro quando comparado a seu único rival, o  $\pi$ . Embora o  $\pi$  seja mais venerável e tenha um grande passado, que chega aos babilônios,  $e$  não é tão oprimido pelo peso da história. A constante  $e$  é jovem e vibrante e está sempre presente quando há “crescimento” envolvido. Seja em populações, dinheiro ou outras quantidades físicas, o crescimento invariavelmente envolve o  $e$ .**

$e$  é o número cujo valor aproximado é 2,71828. Então por que ele é tão especial? Não é um número escolhido ao acaso, mas uma das grandes constantes matemáticas. Veio à luz no início do século XVII, quando diversos matemáticos puseram suas energias no esclarecimento da ideia de um logaritmo, a invenção brilhante que permitiu que a multiplicação de grandes números pudesse ser convertida em soma.

Mas a história começa na verdade com algum “*e-commerce*” do século XVII. Jacob Bernoulli era um dos ilustres Bernoullis da Suíça, uma família que se encarregou de suprir o mundo com uma dinastia de matemáticos. Jacob começou a trabalhar em 1683 com o problema dos juros compostos.

**Dinheiro, dinheiro, dinheiro** Vamos considerar um período de um ano, uma taxa de juros de galopantes 100% e um depósito



inicial (chamado de “principal”) de £1. É claro que raramente conseguimos lucrar 100% sobre nosso dinheiro, mas esse número serve aos nossos propósitos e o conceito pode ser adaptado a taxas de juros como 6% e 7%. Do mesmo modo, se temos um principal maior, como £10.000, podemos multiplicar tudo por 10.000.

No fim do ano, com 100% de juros, teremos o principal e a quantia de juros ganha, que nesse caso é também £1. Assim, teremos a principesca soma de £2. Agora suponhamos que a taxa de juros seja reduzida à metade, 50%, mas seja aplicada separadamente para cada período de meio ano. Para a primeira metade do ano ganhamos juros de 50 pence e nosso principal cresceu a £1,50 no final do primeiro semestre. Assim, ao final do ano inteiro teremos essa quantia e os 75 pence de juros sobre essa soma. Nossa £1 cresceu para £2,25 no fim do ano! A composição dos juros de cada semestre nos daria 25 pence a mais. Pode não parecer muito, mas se tivéssemos £10.000 para investir, teríamos agora £2.200 de juros, em vez de £2.000. Compondo os juros a cada meio ano, ganhamos £250 a mais.

Mas se a composição de juros a cada semestre significa que ganhamos sobre as nossas economias, o banco também vai ganhar sobre qualquer dinheiro que tenhamos – por isso temos de ter cuidado! Suponhamos agora que o ano é dividido em quatro trimestres, aplicando juros de 25% a cada trimestre. Efetuando um cálculo semelhante, descobrimos que nossa £1 cresceu para £2,44141. Nosso dinheiro está aumentando, e com as nossas £10.000, pareceria vantajoso se pudéssemos fatiar o ano e aplicar a percentagem de taxa de juros menor a intervalos

de tempo menores.

Será que nosso dinheiro vai aumentar além de todos os limites e nos fazer milionários? Se continuarmos a dividir o ano em unidades cada vez menores, como mostrado na tabela, esse “processo limitante” mostra que a quantia parece se estabilizar em um número constante. É claro, o único período realista de composição é por dia (e é isso o que os bancos fazem). A mensagem matemática é que esse limite, que os matemáticos chamam de  $e$ , é o quanto £1 cresce se esse acúmulo se der continuamente. Isso é bom ou é ruim? Você sabe a resposta: se estiver economizando, “sim”; se você deve dinheiro, “não”. É uma questão de “*e-learning*”.

Composição a cada...	Soma acumulada
----------------------	----------------

ano

£ 2,00000

---

semestre

£ 2,25000

---

trimestre	£ 2,44141
mês	£ 2,61304

semana

£ 2,69260

---

dia

£ 2,71457

---

hora

£ 2,71813

---



minuto

£ 2,71828

---

**O valor exato de  $e$**  Do mesmo modo que  $\pi$ ,  $e$  é um número irracional, de modo que, como  $\pi$ , não podemos saber seu valor exato. Para 20 casas decimais, o valor de  $e$  é 2,71828182845904523536...

Usando-se apenas frações, a melhor aproximação para o valor de  $e$  é  $87/32$ , se a parte de cima e a de baixo da fração forem limitadas a números com dois algarismos. Curiosamente, se o de cima e o de baixo forem limitados a números de três algarismos, a melhor fração é  $878/323$ . Essa segunda fração é uma espécie de extensão palindrômica da primeira – matemáticos têm um hábito de apresentar essas pequenas surpresas. Uma expansão de série bem conhecida para  $e$  é dada por

$$e = 1 + \frac{1}{1} + \frac{1}{2 \times 1} + \frac{1}{3 \times 2 \times 1} + \frac{1}{4 \times 3 \times 2 \times 1} + \frac{1}{5 \times 4 \times 3 \times 2 \times 1} + \dots$$

A notação fatorial, usando um ponto de exclamação, é útil aqui. Nesse processo, por exemplo,  $5! = 5 \times 4 \times 3 \times 2 \times 1$ . Usando essa notação,  $e$  toma a forma mais familiar de

$$e = 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \frac{1}{4!} + \frac{1}{5!} + \dots$$

Então o número  $e$  certamente parece ter algum padrão. Em suas propriedades matemáticas,  $e$  parece mais “simétrico” do que  $\pi$ .

Se você quiser um meio de decorar as primeiras casas decimais de  $e$ , tente isso: “*We attempt a mnemonic to remember a strategy to memorize this count*” [Tentamos um processo mnemônico para lembrar uma estratégia para decorar essa contagem] em que a contagem das letras de cada palavra dá o algarismo seguinte de

*e*. Se você conhecer a história norte-americana, poderá lembrar que *e* é “2,7 Andrew Jackson Andrew Jackson”, porque Andrew Jackson (“Old Hickory”), o sétimo presidente dos Estados Unidos, foi eleito em 1828. Há inúmeros dispositivos como esse para lembrar de *e*, mas o interesse está mais na curiosidade do que em qualquer vantagem matemática.

O fato de *e* ser irracional (não é uma fração) foi provado por Leonhard Euler em 1737. Em 1840, o matemático francês Joseph Liouville mostrou que *e* não era a solução de qualquer equação quadrática, e em 1873, em um trabalho desbravador, seu compatriota Charles Hermite provou que o *e* é transcendental (não pode ser a solução para qualquer equação algébrica). O importante aqui foi o método usado por Hermite. Nove anos mais tarde, Ferdinand von Lindemann adaptou o método de Hermite para provar que  $\pi$  é transcendental, um problema muito mais vistoso.

Uma questão foi resolvida, mas outras apareceram. Será o *e* elevado à potência *e* transcendental? É uma expressão tão estranha, de que outro jeito ela pode ser? No entanto, isso não foi provado de modo minucioso e, pelos padrões rigorosos da matemática, tem de ser classificada como uma conjectura. Os matemáticos têm avançado lentamente na direção de uma prova e provaram que é impossível que *tanto* essa expressão *como* o *e* elevado à potência  $e^2$  sejam transcendentais. Próximo, mas não próximo o bastante.

As conexões entre  $\pi$  e *e* são fascinantes. Os valores de  $e^\pi$  e de  $\pi^e$  são próximos, mas é facilmente demonstrado (sem na verdade

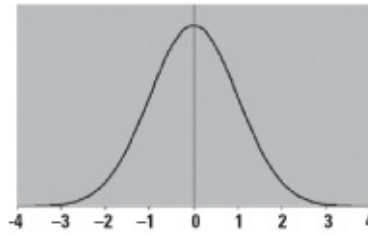
calcular os valores deles) que  $e^\pi > \pi^e$ . Se você “trapacear” e der uma olhada na sua calculadora, verá os valores aproximados de  $e^\pi = 23,14069$  e de  $\pi^e = 22,45916$ . O número  $e^\pi$  é conhecido como constante de Gelfond (em homenagem ao matemático russo Aleksandr Gelfond) e foi demonstrado que é transcendental. Sabe-se muito menos a respeito de  $\pi^e$ ; ainda não se provou que seja irracional – se na verdade o for.

**Será que o  $e$  é importante?** O principal contexto em que o  $e$  é encontrado é em crescimento. Os exemplos são crescimento econômico e o crescimento de populações. Ligadas a isso há curvas que dependem do  $e$ , usadas para modelar o decaimento radioativo.

O número  $e$  também ocorre em problemas sem ligação com o crescimento. Pierre Montmort investigou um problema de probabilidade no século XVIII, que tem sido desde então estudado extensivamente. Na versão mais simples, um grupo de pessoas vai almoçar e depois apanha aleatoriamente seus chapéus. Qual a probabilidade de que ninguém pegue seu próprio chapéu?

Pode-se demonstrar que essa probabilidade é de  $1/e$  (cerca de 37%), de maneira que a probabilidade de pelo menos uma pessoa pegar seu próprio chapéu é de  $1 - 1/e$  (63%). A distribuição de Poisson que lida com eventos raros é outra. Essas são ocorrências iniciais, mas de modo algum isoladas: James Stirling alcançou uma aproximação notável ao valor fatorial  $n!$  envolvendo  $e$  (e  $\pi$ ); em estatística, a conhecida “curva de sino” da distribuição normal envolve  $e$ ; e em engenharia a curva feita

pelo cabo de uma ponte suspensa depende de  $e$ . A lista é infinita.



A distribuição normal.

**Uma identidade de sacudir a terra** O prêmio pela fórmula mais notável de toda a matemática envolve  $e$ . Quando pensamos nos números mais famosos da matemática, pensamos em 0, 1,  $\pi$ ,  $e$  e o número imaginário  $i = \sqrt{-1}$ .

Como pode ser possível que

$$e^{i\pi} + 1 = 0$$

E é! Esse resultado é atribuído a Euler.

Talvez a importância real de  $e$  resida no mistério com que ele cativou gerações de matemáticos. Em resumo,  $e$  é inevitável. Exatamente por que um autor como E.V. Wright se deu ao trabalho de escrever um romance “*e-less*” – supostamente ele também tem um pseudônimo – mas o seu *Gadsby* é exatamente isso. É difícil imaginar um matemático se pondo a escrever um livro-texto “*e-less*”, ou sendo capaz de escrevê-lo.

**A ideia condensada:  
o mais natural dos números**



# 07 Infinito

## linha do tempo

350 d.C.	1639	1655	1874	Década de 1960
Aristóteles rejeita um infinito real	Girard Desargues introduz o conceito de infinitude na geometria	John Wallis é creditado como sendo o primeiro a usar o "nó do amor", o símbolo $\infty$ , para infinito	Cantor trata a ideia de infinito com rigor, especificando diversas ordens de infinito	Abraham Robinson elabora uma aritmética não padrão baseada na ideia de infinitesimal

**Qual é o tamanho do infinito? A resposta curta é  $\infty$  (o símbolo do infinito). Pense em uma linha reta com números cada vez maiores dispostos ao longo dela, se esticando “até o infinito”. Para cada número enorme produzido, digamos  $10^{1.000}$ , haverá sempre um maior, tal que  $10^{1.000} + 1$ .**

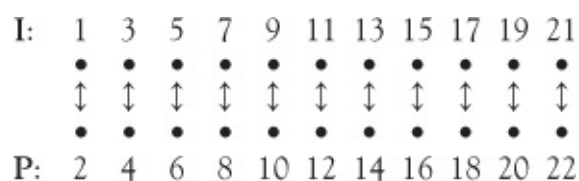
Essa é uma ideia tradicional de infinito, com números avançando para sempre. A matemática usa o infinito de muitas maneiras, mas é preciso tomar cuidado ao tratar o infinito como um número comum. Não é.

**Contando** O matemático alemão Georg Cantor nos deu um conceito inteiramente diferente do infinito. No processo, ele sozinho criou uma teoria que tem incentivado grande parte dos matemáticos modernos. A ideia da qual depende a teoria de Cantor tem a ver com a noção primitiva de contagem, mais simples do que a que usamos hoje nos negócios do dia a dia.

Imagine um fazendeiro que não conheça a contagem com números. Como saberia ele quantos carneiros tem? Simples – quando deixa os carneiros saírem pela manhã, ele pode saber se todos voltaram à noite pareando cada carneiro com uma pedra, tirada de uma pilha na porteira de seu pasto. Se algum carneiro

for perdido, haverá uma pedra sobrando. Mesmo sem usar números, o fazendeiro está sendo muito matemático. Ele está usando a ideia de correspondência um a um entre carneiros e pedras. Essa ideia primitiva apresenta algumas consequências surpreendentes.

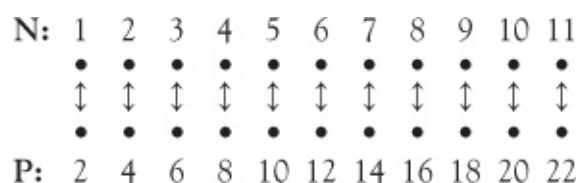
A teoria de Cantor envolve conjuntos (um conjunto é simplesmente uma coleção de objetos). Por exemplo,  $N = \{1, 2, 3, 4, 5, 6, 7, 8, \dots\}$  significa o conjunto (positivo) de números inteiros. Uma vez que temos um conjunto, podemos falar de subconjuntos, que são conjuntos menores dentro do conjunto maior. Os subconjuntos mais evidentes ligados ao nosso exemplo  $N$  são os subconjuntos  $O = \{1, 3, 5, 7, \dots\}$  e  $E = \{2, 4, 6, 8, \dots\}$ , que são os conjuntos dos números ímpares e dos pares, respectivamente. Se tivéssemos de perguntar “existe a mesma quantidade de números ímpares que de números pares?”, o que responderíamos? Embora não seja possível fazer isso contando os elementos em cada conjunto e comparando as respostas, a resposta mesmo assim seria “sim”. Em que está baseada essa confiança? – provavelmente em alguma coisa do tipo “metade dos números inteiros é ímpar e metade é par”. Cantor concordaria com a resposta, mas daria um motivo diferente. Ele diria que cada vez que temos um número ímpar, temos um “companheiro” par ao lado dele. A ideia de que os dois conjuntos  $O$  e  $E$  têm o mesmo número de elementos é baseada no pareamento de cada número ímpar com um número par:





Se tivermos de fazer a próxima pergunta “a quantidade de números inteiros é igual à de números *pares*?”, a resposta poderá ser “não”, e o argumento é de que o conjunto  $N$  tem o dobro dos números do conjunto de números somente pares.

A noção de “mais”, contudo, é um tanto nebulosa quando estamos lidando com conjuntos que contêm um número indefinido de elementos. Seria melhor a ideia de correspondência um a um. Surpreendentemente há uma correspondência biunívoca entre  $N$  e o conjunto de números pares  $E$ :



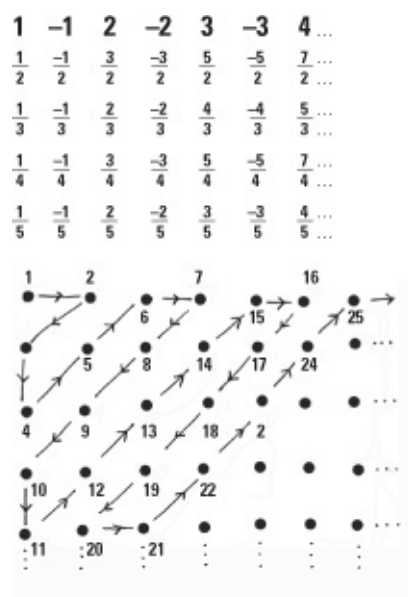
Chegamos à assombrosa conclusão de que existe a “mesma quantidade” de números inteiros e de números pares! Isso vai de encontro com a “noção comum” declarada pelos gregos antigos; o início do texto dos *Elementos* de Euclides de Alexandria diz que “o todo é maior que a parte”.

**Cardinalidade** O número de elementos em um conjunto é chamado de sua “cardinalidade”. No caso dos carneiros, a cardinalidade registrada pelos contadores do fazendeiro é 42. A cardinalidade do conjunto  $\{a, b, c, d, e\}$  é 5 e é escrito como  $\text{card} \{a, b, c, d, e\} = 5$ . Então a cardinalidade é uma medida do “tamanho” de um conjunto. Para a cardinalidade dos números inteiros  $N$  e de qualquer correspondência biunívoca com  $N$ , Cantor usou o símbolo  $\aleph_0$  ( $\aleph$ , ou “aleph”, vem do alfabeto hebraico; o símbolo  $\aleph_0$  é lido como “aleph zero”). Então, na

linguagem matemática, podemos escrever  $\text{card}(\mathbf{N}) = \text{card}(\mathbf{I}) = \text{card}(\mathbf{P}) = \aleph_0$ .

Qualquer conjunto que possa ser posto em uma correspondência biunívoca com  $\mathbf{N}$  é chamado de conjunto “contável infinito”. Ser contável infinito significa que podemos escrever os elementos do conjunto em uma lista. Por exemplo, a lista dos números ímpares é simplesmente 1, 3, 5, 7, 9,... e sabemos qual é o primeiro elemento, qual é o segundo, e daí por diante.

**Serão as frações contáveis infinitas?** O conjunto das frações  $\mathbf{Q}$  é um conjunto maior do que  $\mathbf{N}$  no sentido de que  $\mathbf{N}$  pode ser considerado como um subconjunto de  $\mathbf{Q}$ . É possível anotar todos os elementos de  $\mathbf{Q}$  em uma lista? Dá para delinear uma lista de modo que cada fração (inclusive as negativas) esteja nela, de alguma maneira? A ideia de que um conjunto tão grande possa ser posto em uma correspondência biunívoca com  $\mathbf{N}$  parece impossível. No entanto, isso pode ser feito.

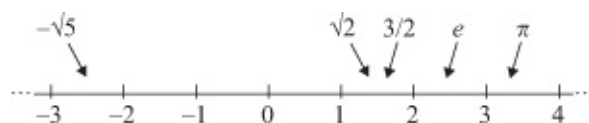


O jeito de começar isso é pensar em termos de duas dimensões.

De início, escrevemos uma linha de todos os números inteiros, positivos e negativos, alternadamente. Embaixo dessa linha escrevemos todas as frações com 2 no denominador, mas omitimos aquelas que aparecem na linha de cima (como  $6/2$ ). Abaixo dessa linha escrevemos as frações que tenham 3 como denominador, outra vez omitindo as que já foram anotadas. Continuamos desse modo, sem acabar nunca, é claro, mas sabendo exatamente onde cada fração aparece no diagrama. Por exemplo,  $209/67$  está na  $67^{\text{a}}$  linha, cerca de 200 casas à direita de  $1/67$ .

Ao exibir todas as frações desse jeito, pelo menos potencialmente, podemos construir uma lista unidimensional. Se começarmos na linha de cima e passarmos para a direita a cada passo, jamais chegaremos à segunda linha. Entretanto, ao escolher um caminho tortuoso, em ziguezague, podemos ter sucesso. Começando com 1, a lista linear prometida começa: 1,  $-1$ ,  $1/2$ ,  $1/3$ ,  $-1/2$ , 2,  $-2$ , e segue as setas. Cada fração, positiva ou negativa, está de alguma maneira na lista linear, e inversamente, sua posição dá seu “companheiro” na lista bidimensional de frações. Então, podemos concluir que o conjunto de frações  $\mathbb{Q}$  é contável infinito e escrevemos  $\text{card}(\mathbb{Q}) = \aleph_0$ .

**Listar os números reais** Embora as frações expliquem muitos elementos da linha dos números reais, há também números reais como  $\sqrt{2}$ ,  $e$  e  $\pi$  que *não* são frações. Esses são os números irracionais – eles “preenchem as lacunas” para nos dar a real linha número  $\mathbb{R}$ .



Com as lacunas preenchidas, o conjunto  $\mathbf{R}$  é chamado de “continuum”. Então, como podemos fazer uma lista dos números reais? Em uma jogada de puro brilhantismo, Cantor demonstrou que até mesmo uma tentativa de botar os números reais entre 0 e 1 em uma lista está fadada ao fracasso. Isso sem dúvida virá como um choque para pessoas que já são viciadas em fazer listas, e elas podem realmente ficar pensando como é que um conjunto de números não pode ser anotado, um número após o outro.

Suponhamos que você não acredite em Cantor. Você sabe que cada número entre 0 e 1 pode ser expresso como uma dízima, uma extensão decimal, por exemplo,  $1/2 = 0,50000000000000...$  e  $1/\pi = 0,31830988618379067153...$  e você terá de dizer a Cantor, “aqui está a minha lista de todos os números entre 0 e 1”, que chamaremos de  $r_1, r_2, r_3, r_4, r_5, \dots$ . Se você não conseguir produzir uma, então Cantor estaria certo.

Imagine que Cantor olhe para sua lista e marque em **negrito** os números na diagonal:

$r_1$ : 0,  **$a_1$** ,  $a_2$ ,  $a_3$ ,  $a_4$ ,  $a_5$ ...  
 $r_2$ : 0,  $b$ ,  $b_1$ ,  **$b_2$** ,  $b_3$ ,  $b_4$ ,  $b_5$ ,...  
 $r_3$ : 0,  $c$ ,  $c_1$ ,  $c_2$ ,  $c_3$ ,  **$c_4$** ,  $c_5$ ,...  
 $r_4$ : 0,  $d$ ,  $d_1$ ,  $d_2$ ,  $d_3$ ,  $d_4$ ,  **$d_5$** ,...

Cantor diria, “tudo bem, mas onde está o número  $x = x_1, x_2, x_3, x_4, x_5, \dots$  onde  $x_1$  difere de  $a_1$ ,  $x_2$  difere de  $b_2$ ,  $x_3$  difere de  $c_3$ , seguindo

pela diagonal abaixo? O  $x$  dele difere de cada número na sua lista em uma casa decimal, e então não pode estar ali. Cantor tem razão.

Na verdade, não há lista possível para o conjunto de números reais  $\mathbf{R}$ , de modo que é um conjunto infinito “maior”, um conjunto com uma “ordem de infinitude mais alta” do que a infinitude do conjunto de frações  $\mathbf{Q}$ . O grande simplesmente ficou maior.

**A ideia condensada:  
uma chuva  
de infinitudes**

## 08 Números imaginários

### linha do tempo

1572 d.C.	1777	1806	1811	1837
Rafael Bombelli faz cálculos com números imaginários	Euler usa pela primeira vez o símbolo $i$ para representar a raiz quadrada de $-1$	A representação diagramática de Argand leva o nome de "diagrama de Argand"	Carl Friedrich Gauss trabalha com funções de variáveis complexas	William R. Hamilton trata números complexos como pares ordenados de números reais

**Certamente conseguimos imaginar números. Algumas vezes imagino que a minha conta bancária tem um crédito de um milhão de libras esterlinas e não há dúvidas de que isso seria um “número imaginário”. Mas o uso matemático do imaginário não tem nada a ver com sonhar acordado.**

Pensa-se que o rótulo “imaginário” se deve ao filósofo e matemático René Descartes, ao reconhecer soluções curiosas de equações que definitivamente não eram números ordinários. Será que os números imaginários existem ou não? Essa foi uma questão discutida por filósofos enquanto se concentravam na palavra “imaginária”. Para os matemáticos, a existência de números imaginários não é problema. Eles fazem tanto parte da vida diária quanto o número 5 ou  $\pi$ . Números imaginários podem não ajudá-lo quando vai às compras, mas pergunte a um projetista de aviões ou a um engenheiro elétrico e você vai descobrir que eles têm uma importância vital. E somando um número real com um imaginário obtemos aquilo que é chamado de número “complexo”, que imediatamente parece menos filosoficamente problemático. A teoria dos números complexos gira em torno da raiz quadrada de  $-1$ . Então que número, ao ser elevado ao quadrado, nos dá  $-1$ ?

Se tomar qualquer número não zero e multiplicá-lo pelo seu próprio valor (elevá-lo ao quadrado), você sempre vai obter um número positivo. Dá para acreditar nisso quando elevamos ao quadrado números positivos, mas será verdadeiro se elevarmos números negativos ao quadrado? Podemos usar  $-1 \times -1$  como um caso a ser testado. Mesmo se tivermos esquecido da regra escolar de que “dois negativos produzem um positivo”, é possível lembrar que a resposta é ou  $-1$  ou  $+1$ . Se achássemos que  $-1 \times -1$  era igual a  $-1$ , poderíamos dividir cada lado por  $-1$  e acabar com a conclusão de que  $-1 = 1$ , o que é absurdo. Então temos de concluir que  $-1 \times -1 = 1$ , que é positivo. O mesmo argumento pode ser usado para outros números negativos, além de  $-1$ , portanto, quando qualquer número real é elevado ao quadrado, o resultado nunca pode ser negativo.

## Construindo $\sqrt{-1}$

Até mesmo os engenheiros, um pessoal muito prático, encontraram usos para números complexos. Quando Michael Faraday descobriu a corrente alternada nos anos 1830, os números imaginários ganharam uma realidade física. Nesse caso, a letra  $j$  é usada para representar  $\sqrt{-1}$  em vez de  $i$ , porque  $i$  corresponde a corrente elétrica.

Isso provocou um certo impasse nos anos iniciais dos números complexos no século XVI. Quando o impasse foi resolvido, a solução liberou a matemática das algemas dos números comuns e abriu um vasto campo de inquirição, nunca antes sonhado. O desenvolvimento dos números complexos é a “finalização dos

números reais” para um sistema naturalmente mais perfeito.

**A raiz quadrada de  $-1$**  Já vimos que, restrita à linha de números reais,



não há nenhuma raiz quadrada de  $-1$ , já que o quadrado de número algum pode ser negativo. Se continuarmos a pensar em números apenas na linha dos números reais, podemos muito bem desistir, continuar a chamá-los de números imaginários, ir tomar uma xícara de chá com os filósofos e não ter mais nada a ver com eles. Ou podemos dar o passo ousado de aceitar como uma nova entidade, que denotaremos por  $i$ .

Com esse ato mental, os números imaginários realmente existem. Não sabemos o que eles são, mas acreditamos em sua existência. Pelo menos sabemos que  $i^2 = -1$ . Então em nosso novo sistema de números temos todos os nossos velhos amigos, como os números reais  $1, 2, 3, 4, \pi, e, \sqrt{2}, +2i, e + \pi i$  e daí por diante.

Esse importante passo na matemática foi tomado por volta do início do século XIX, quando fugimos da linha unidimensional de números para um estranho novo plano de números bidimensional.

**Soma e multiplicação** Agora que temos os números complexos em mente, números com a forma  $a + bi$ , o que podemos fazer com eles? Do mesmo modo que os números reais, eles podem ser somados e multiplicados.

Podemos somá-los adicionando suas partes respectivas. Então 2



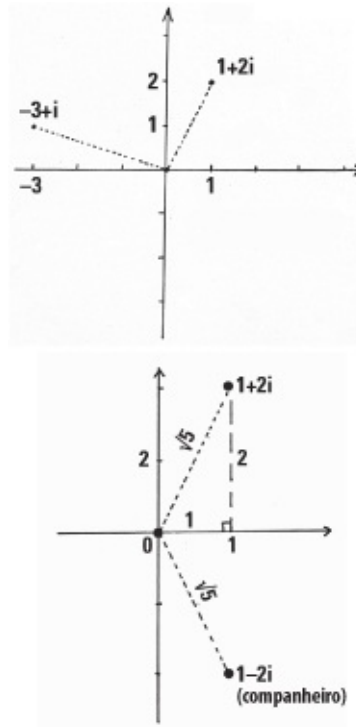
+  $3i$  somados a  $8 + 4i$  dá  $(2 + 8) + (3 + 4)i$ , resultando em  $10 + 7i$ .

A multiplicação é quase tão simples quanto. Se quisermos multiplicar  $2 + 3i$  por  $8 + 4i$ , primeiro multiplicamos cada par de símbolos

$$(2 + 3i) \times (8 + 4i) = (2 \times 8) + (2 \times 4i) + (3i \times 8) + (3i \times 4i)$$

e somamos os termos resultantes,  $16$ ,  $8i$ ,  $24i$  e  $12i^2$  (nesse último termo substituímos  $i^2$  por  $-1$ ). O resultado da multiplicação é, portanto,  $(16 - 12) + (8i + 24i)$  que é o número complexo  $4 + 32i$ .

Com os números complexos, todas as regras normais da aritmética são obedecidas. Subtração e divisão são sempre possíveis (exceto pelo número complexo  $0 + 0i$ , mas isso também não era permitido para zero nos números reais). Na verdade, os números complexos gozam de todas as propriedades dos números reais menos uma. Não podem ser divididos em positivos e negativos como no caso dos números reais.



**O diagrama de Argand** A bidimensionalidade dos números complexos é claramente vista quando eles são representados em um diagrama. Os números complexos  $-3 + i$  e  $1 + 2i$  podem ser traçados no que chamamos de diagrama de Argand: esse modo de representar números complexos foi batizado em homenagem a Jean Robert Argand, um matemático suíço, embora outros tivessem uma notação semelhante por volta da mesma época.

Cada número complexo tem um “companheiro” oficialmente chamado de seu “conjugado”. O companheiro de  $1 + 2i$  é  $1 - 2i$ , encontrado invertendo o sinal na frente do segundo componente. O companheiro de  $1 - 2i$ , do mesmo modo, é  $1 + 2i$ , de maneira que é um companheirismo verdadeiro.

A soma e a multiplicação de companheiros sempre produzem um número real. No caso de somar  $1 + 2i$  e  $1 - 2i$  obtemos 2, e quando os multiplicamos obtemos 5. Essa multiplicação é mais

interessante. A resposta 5 é o quadrado do “comprimento” do número complexo  $1 + 2i$  e isso é igual ao comprimento de seu companheiro. Pondo de outra forma, poderíamos definir o comprimento de um número complexo como

$$\text{comprimento de } w = \sqrt{(w \times \text{companheiro de } w)}$$

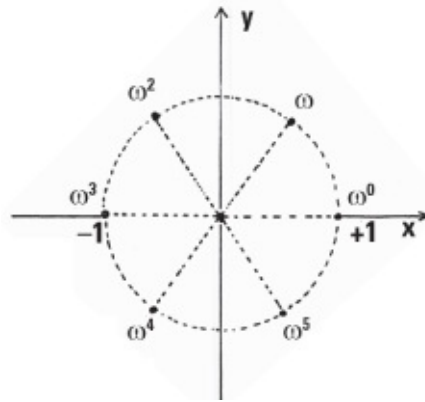
Verificando isso para  $-3 + i$  encontramos que o comprimento de  $(-3 + i) = \sqrt{(-3+i \times -3 -i) = \sqrt{(9 + 1)}$ , então o comprimento de  $(-3 + i) = \sqrt{10}$ .

A separação de números complexos do misticismo deve muito a sir William Rowan Hamilton, o principal matemático da Irlanda no século XIX. Ele reconheceu que na verdade não se precisava de  $i$  para a teoria. Ele só funcionava como um símbolo para representar qualquer coisa e podia ser jogado fora. Hamilton considerava um número complexo como um “par ordenado” de números reais  $(a, b)$ , exibindo sua qualidade bidimensional e não recorrendo ao místico  $\sqrt{-1}$ . Cortado o  $i$ , a soma passa a ser

$$(2, 3) + (8, 4) = (10, 7),$$

e, um pouco menos evidente, a multiplicação é

$$(2, 3) \times (8, 4) = (4, 32)$$



A inteireza do sistema de números complexos se torna mais clara quando pensamos no que é chamado de “*enésima raiz da unidade*” (para os matemáticos “unidade” significa “um”). São as soluções para a equação  $z^n = 1$ . Vamos tomar  $z^6 = 1$  como exemplo. Há duas raízes  $z = 1$  e  $z = -1$  na linha dos números reais – porque  $1^6 = 1$  e  $(-1)^6 = 1$  –, mas onde estão as outras, quando certamente deveriam haver seis? Do mesmo modo como em duas raízes reais, todas as seis raízes têm a unidade como comprimento e são encontradas no círculo com centro na origem e cujo raio é a unidade.

Há ainda mais verdades. Se olharmos para  $w = 1/2 + \sqrt{3}/2i$ , que é a raiz no primeiro quadrante, as raízes sucessivas (na direção anti-horária) são  $w^2, w^3, w^4, w^5, w^6 = 1$  e ficam nos vértices de um hexágono regular. Em geral, cada uma das  $n$  raízes da unidade vai ficar no círculo e pode ficar nos cantos, ou “vértices”, de uma forma ou polígono regular de  $n$  lados.

**Estendendo números complexos** Uma vez que os matemáticos obtiveram os números complexos, eles instintivamente pensaram em generalizações. Números complexos são bidimensionais, mas o que há de especial em relação ao 2?

Durante anos, Hamilton procurou construir números tridimensionais e elaborou um jeito de os somar e multiplicar, mas só teve sucesso quando passou para quatro dimensões. Logo depois esses números com quatro dimensões foram, eles próprios, generalizados para oito dimensões (chamados números de Cayley). Muitos imaginaram números de 16 dimensões como uma possível continuação da história – mas 50 anos depois do importante feito de Hamilton eles se mostraram impossíveis.

## **A ideia condensada: números irreais com usos reais**

# 09 Primos

## linha do tempo

300 a.C.	230 a.C.	1742 d.C.	1896	1966
O <i>Elementos</i> de Euclides fornece uma prova de que o número de primos é infinito	Eratóstenes de Cirene descreve um método de peneirar números primos entre os números inteiros (Crivo de Eratóstenes)	Goldbach especula que todo número par (maior que 2) é a soma de dois primos	É provado o teorema do número primo sobre a distribuição de primos	Chen Jingrun quase confirma a conjectura de Goldbach

**A matemática é um assunto tão maciço, entrelaçando-se com todas as vias da atividade humana, que às vezes pode parecer esmagadora. Ocasionalmente, precisamos voltar ao básico. Isso invariavelmente significa um retorno aos números inteiros 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12... Pode haver algo mais básico do que isso?**

Bem,  $4 = 2 \times 2$  e então podemos parti-lo em componentes primários. Podemos quebrar algum outro número? Na verdade, há mais alguns:  $6 = 2 \times 3$ ,  $8 = 2 \times 2 \times 2$ ,  $9 = 3 \times 3$ ,  $10 = 2 \times 5$ ,  $12 = 2 \times 2 \times 3$ . Esses são números compostos porque eles são construídos a partir dos muito básicos 2, 3, 5, 7... Os números “inquebráveis” são os números 2, 3, 5, 7, 11, 13... Esses são os “números primos”, ou simplesmente “primos”. Um primo é um número que só é divisível por 1 e por ele mesmo. Você pode ficar pensando então se o próprio 1 é um número primo. De acordo com essa definição, deveria ser, e na verdade muitos matemáticos importantes no passado trataram o 1 como primo, mas matemáticos modernos começam seus primos com 2. Isso permite que seus teoremas sejam enunciados de modo elegante. Para nós, também, o número 2 é o primeiro primo.

Para os primeiros poucos números inteiros podemos sublinhar os primos: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18,

19, 20, 21, 22, 23... O estudo dos números primos nos leva de volta ao mais básico do básico. Os números primos são importantes por serem os “átomos” da matemática. Do mesmo modo que os elementos básicos dos quais todos os outros compostos químicos são derivados, pode se construir a partir dos números primos para criar compostos matemáticos.

O resultado matemático que consolida isso tudo tem o nome grandioso de “teorema de decomposição de número primo”. Isso diz que qualquer número inteiro maior do que 1 pode ser escrito multiplicando-se exatamente números primos de um jeito específico. Vimos que  $12 = 2 \times 2 \times 3$  e que não há outra maneira de fazer isso com componentes primos. Isso é frequentemente escrito na notação de potência:  $12 = 2^2 \times 3$ . Em outro exemplo, 6.545.448 pode ser escrito  $2^2 \times 3^5 \times 7 \times 13 \times 37$ .

0	1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18	19
20	21	22	23	24	25	26	27	28	29
30	31	32	33	34	35	36	37	38	39
40	41	42	43	44	45	46	47	48	49
50	51	52	53	54	55	56	57	58	59
60	61	62	63	64	65	66	67	68	69
70	71	72	73	74	75	76	77	78	79
80	81	82	83	84	85	86	87	88	89
90	91	92	93	94	95	96	97	98	99

**Descoberta dos primos** Infelizmente não existe um conjunto de fórmulas para a identificação de primos, e parece não haver nenhum padrão no aparecimento deles entre os números inteiros. Um dos primeiros métodos para os encontrar foi desenvolvido por um contemporâneo mais jovem de Arquimedes que passou grande parte de sua vida em Atenas, Eratóstenes de Cirene. Seu cálculo preciso do comprimento do equador foi muito admirado em sua própria época. Hoje ele é conhecido por

sua peneira (crivo) para encontrar números primos. Eratóstenes imaginou os números contáveis estendidos à sua frente. Ele sublinhou o 2 e cortou fora todos os múltiplos de 2. Depois passou para o 3, sublinhou-o e cortou todos os múltiplos de 3. Continuando desse modo, ele passou todos os compostos pelo crivo. Os números sublinhados deixados para trás na peneira eram os primos.

Desse modo podemos prever primos, mas como decidimos se um dado número é primo ou não? Que tal 19.071 ou 19.073? A não ser pelos primos 2 e 5, um número primo deve terminar em 1, 3, 7 ou 9, mas essa exigência não é suficiente para fazer com que um número seja primo. É difícil saber se um número grande terminado em 1, 3, 7 ou 9 é primo ou não sem tentar fatores possíveis. Aliás,  $19.071 = 3^2 \times 13 \times 163$ , não é primo, mas 19.073 é.

Outro desafio tem sido descobrir qualquer padrão na distribuição dos primos. Vamos ver quantos primos há em cada segmento de 100 entre 1 e 1.000.

Limite	1-100	101-200	201-300	301-400	401-500	501-600	601-700	701-800	801-900	901-1.000	1-1.000
Número de primos	25	21	16	16	17	14	16	14	15	14	168

Em 1792, com apenas 15 anos de idade, Carl Friedrich Gauss sugeriu uma fórmula  $P(n)$  para estimar o número de primos menor do que um dado número  $n$  (isso é agora chamado o teorema do número primo). Para  $n = 1.000$  a fórmula dá o valor aproximado de 172. O número real de primos, 168, é menor do que essa estimativa. Sempre se supôs que esse era o caso para qualquer valor de  $n$ , mas os primos muitas vezes guardam surpresas e já foi demonstrado que para  $n = 10^{371}$  (um número



enorme escrito à mão por extenso como 1 seguido de 371 zeros) o número real de primos *excede* a estimativa. Na verdade, em algumas regiões dos números inteiros, a diferença entre a estimativa e o número verdadeiro oscila entre menos e excesso.

**Quantos?** Há uma infinidade de números primos. Euclides declarou em seus *Elementos* (Livro 9, proposição 20) que os “números primos são em maior número do que qualquer multidão atribuída a números primos”. A bela prova de Euclides segue assim:

Suponha que  $P$  é o maior primo, e considere o número  $N = (2 \times 3 \times 5 \times \dots \times P) + 1$ . Ou o  $N$  é primo ou não é. Se  $N$  for primo, produzimos um primo maior do que  $P$ , o que é uma contradição à nossa suposição. Se  $N$  não é um primo, ele deve ser divisível por algum primo, digamos  $p$ , que é um de 2, 3, 5, ...,  $P$ . Isso significa que  $N - (2 \times 3 \times 5 \times \dots \times P)$  é divisível por  $p$ . Mas este número é igual a 1 e então 1 é divisível por  $p$ . Isso é impossível, já que todos os primos são maiores que 1. Então, não importa a natureza de  $N$ , chegamos a uma contradição. Nossa suposição original de haver um número primo maior que  $P$  é, portanto, falsa. Conclusão: o número de primos é ilimitado.

Embora os primos se “estendam até o infinito”, esse fato não impediu que as pessoas tentassem encontrar o maior número primo conhecido. O detentor do recorde mais recente é o enorme primo de Mersenne  $2^{24036583} - 1$ , que é aproximadamente  $10^{7235732}$  ou um número começado com 1 seguido por 7.235.732 zeros.

**O desconhecido** Importantes áreas desconhecidas que têm

relação com os números primos são o “problema dos primos gêmeos” e a famosa “conjectura de Goldbach”.

Os primos gêmeos são pares de primos consecutivos separados apenas por um número par. Os primos gêmeos vão de 1 a 100 e são 3, 5; 5, 7; 11, 13; 17, 19; 29, 31; 41, 43; 59, 61; 71, 73. Na linha de frente numérica, sabe-se que há 27.412.679 gêmeos, menos de  $10^{10}$ . Isso significa que os números pares com gêmeos, como 12 (que tem os gêmeos 11, 13), constituem apenas 0,274% dos números nesse intervalo. Haverá um número infinito de primos gêmeos? Seria curioso se não houvesse, mas ninguém até agora conseguiu demonstrar uma prova disso.

Christian Goldbach conjecturou que:

*Todo número par maior do que 2 é a soma de dois números primos.*

Por exemplo, 42 é um número par e podemos escrevê-lo como 5 + 37. O fato de que podemos também escrevê-lo como 11 + 31, 13 + 29 ou 19 + 23 não importa – só precisamos de *um* jeito. A conjectura é verdadeira para uma gama enorme de números – mas nunca foi provada em geral. Entretanto, houve progresso, e alguns acham que a prova não está longe. O matemático chinês Chen Jingrun deu um grande passo. Seu teorema declara que todo número par suficientemente grande pode ser escrito como a soma de um primo e um *semiprimo* (um número que é a multiplicação de dois primos).

## O número do numerologista

Uma das áreas mais desafiadoras da teoria dos números diz respeito ao

“problema de Waring”. Em 1770, Edward Waring, um professor de Cambridge, apresentou problemas envolvendo a escrita de números inteiros, como adição de potências. Nesse conjunto, as artes mágicas da numerologia se encontram com a ciência clínica da matemática no formato de primos, somas de quadrados e somas de cubos. Na numerologia, considere o inigualável número místico 666, o “número da besta” no livro bíblico do *Apocalipse*, e que apresenta algumas propriedades inesperadas. Ele é a soma dos quadrados dos sete primeiros primos:

$$666 = 2^2 + 3^2 + 5^2 + 7^2 + 11^2 + 13^2 + 17^2$$

Os numerólogos estarão também ansiosos por chamar atenção de que ele é a soma de cubos palindrômicos e, se isso não bastar, a pedra fundamental  $6^3$  é a abreviação de  $6 \times 6 \times 6$ .

$$666 = 1^3 + 2^3 + 3^3 + 4^3 + 5^3 + 6^3 + 5^3 + 4^3 + 3^3 + 2^3 + 1^3$$

O número 666 é realmente o “número do numerologista”.

O grande teórico dos números Pierre de Fermat provou que primos da forma  $4k + 1$  podem ser expressos como a soma de dois quadrados em exatamente uma forma (p. ex.,  $17 = 1^2 + 4^2$ ), enquanto aqueles da forma  $4k + 3$  (como 19), não podem ser escritos como a soma de dois quadrados de jeito algum. Joseph Lagrange também provou um famoso teorema matemático a respeito das potências quadradas: todo número inteiro positivo é a soma de quatro quadrados. Então, por exemplo,  $19 = 1^2 + 1^2 + 1^2 + 4^2$ . Potências mais altas foram exploradas e livros foram recheados de teoremas, mas ainda permanecem muitos

problemas.

Descrevemos os números primos como os “átomos da matemática”. Mas “certamente”, dirá você, “os físicos foram além de átomos para unidades ainda mais fundamentais, como os quarks. Será que a matemática parou?”. Se nos limitarmos aos números inteiros, 5 é um número primo e sempre será. Mas Gauss fez uma descoberta de mais longo alcance, que para alguns primos, como 5,  $5 = (1 - 2i) \times (1 + 2i)$ , onde  $i = \sqrt{-1}$  do sistema de números imaginários. Como produto de dois inteiros gaussianos, 5 e números como ele não são indivisíveis como já supomos.

**A ideia condensada:  
os átomos da  
matemática**

# 10 Números perfeitos

## linha do tempo

525 a.C.	300 a.C.	100 d.C.	1603	2006
Os pitagóricos são associados tanto aos números perfeitos quanto aos abundantes	O livro 9 dos <i>Elementos</i> de Euclides discute os números perfeitos	Nicômaco de Gerasa dá uma classificação de números baseada nos números perfeitos	Pietro Cataldi encontra o sexto e o sétimo números perfeitos, $2^{16}(2^{17} - 1) = 8.589.869.056$ e $2^{18}(2^{19} - 1) = 137.438.691.328$	O grande projeto de busca pelo primo encontra o 44º primo de Mersenne (com quase 10 milhões de algarismos) e ainda mais um novo número perfeito pode ser gerado

**Na matemática, a busca pela perfeição tem levado seus aspirantes a diversas situações. Há quadrados perfeitos, mas aqui o termo não é usado no sentido estético. É mais para avisar que existem quadrados imperfeitos. Em outra direção, alguns números têm poucos divisores e alguns têm muitos. No entanto, como na história dos três ursinhos, alguns números são “do jeito certo”. Quando a soma dos divisores de um número é igual ao número propriamente dito, diz-se que ele é perfeito.**

O filósofo grego Espeusipo, que assumiu a direção da Academia depois de seu tio Platão, declarou que os pitagóricos acreditavam que o 10 tem as credenciais certas para a perfeição. Por quê? Porque a quantidade de números primos entre 1 e 10 (ou seja, 2, 3, 5, 7) se igualava à quantidade de não primos (4, 6, 8, 9), e esse era o menor número com essa propriedade. Algumas pessoas têm ideias estranhas sobre a perfeição.

Parece que os pitagóricos na verdade tinham um conceito mais rico de número perfeito. As propriedades matemáticas dos números perfeitos foram delineadas por Euclides no *Elementos* e foram estudadas em profundidade por Nicômaco 400 anos mais tarde, levando a números amigáveis e até a números sociáveis.

Essas categorias foram definidas em termos dos relacionamentos entre eles e seus divisores. Em algum momento eles surgiram com a teoria dos números superabundantes e dos números deficientes e isso os levou ao conceito da perfeição.

O que determina se um número é superabundante são seus divisores e um jogo entre multiplicação e adição. Tome o número 30 e considere seus divisores, ou seja, todos os números que o dividem exatamente e que são menores do que 30. Para números pequenos como o 30, podemos ver que os divisores são 1, 2, 3, 5, 6, 10 e 15. Somando todos esses divisores, obtemos 42. O número 30 é superabundante porque a soma de seus divisores (42) é maior do que o próprio 30.

Classificação	1	2	3	4	5	6	7
Número perfeito.	6	28	496	8.128	33,550,336	8.589.869.056	137.438.691.328

Os primeiros números perfeitos

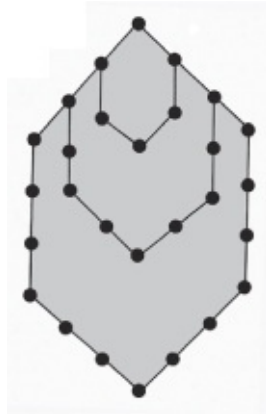
Um número será deficiente se o oposto for verdadeiro – se a soma de seus divisores for menor do que ele próprio. Então o número 26 é deficiente porque seus divisores 1, 2 e 13 somam apenas 16, que é menor do que 26. Os números primos são muito deficientes porque a soma de seus divisores é sempre apenas 1.

Um número que não seja nem superabundante nem deficiente é perfeito. A soma dos divisores de um número perfeito é igual ao próprio número. O primeiro número perfeito é 6. Seus divisores são 1, 2, 3, e, quando os somamos, o resultado é 6. Os pitagóricos ficaram tão encantados com o número 6 e com o modo como suas partes se ajustam que o chamaram de “casamento, saúde e

beleza”. Há uma outra história ligada com o 6, contada por Santo Agostinho (354-430). Ele acreditava que a perfeição do 6 já existia antes da existência do mundo e que o mundo foi criado em 6 dias porque o número era perfeito.

O próximo número perfeito é o 28. Seus divisores são 1, 2, 4, 7 e 14 e, quando os somamos, obtemos 28. Esses dois primeiros números perfeitos, 6 e 28, são um tanto especiais na tradição dos números perfeitos, já que se pode provar que todos os números perfeitos pares terminam em 6 ou 28. Depois do 28, você vai esperar até o 496 para o número perfeito seguinte. É fácil verificar que ele é realmente a soma de seus divisores:  $496 = 1 + 2 + 4 + 8 + 16 + 31 + 62 + 124 + 248$ . Para os números perfeitos seguintes, temos de começar a ir para a estratosfera numérica. Os cinco primeiros eram conhecidos no século XVI, mas ainda não sabemos se existe um maior ou se eles continuam sem limites. O saldo das opiniões sugere que eles, como os primos, continuam para sempre.

Os pitagóricos eram chegados a conexões geométricas. Se tivermos um número perfeito de contas, elas podem ser arrumadas em um colar hexagonal. No caso do 6, isso é o simples hexágono com as contas postas nos vértices, mas para números perfeitos maiores vamos ter de acrescentar subcolares menores dentro do colar maior.



Potência	Resultado	Se resta 1 (Número de Mersenne)	Número primo?
2	4	3	primo
3	8	7	primo
4	16	15	não primo
5	32	31	primo
6	64	63	não primo
7	128	127	primo
8	256	255	não primo
9	512	511	não primo
10	1.024	1.023	não primo
11	2.048	2.047	não primo
12	4.096	4.095	não primo
13	8.192	8.191	primo
14	16.384	16.383	não primo
15	32.768	32.767	não primo

**Números de Mersenne** A chave para construir números perfeitos é uma coleção de números batizados em homenagem ao padre Marin Mersenne, um monge francês que estudou em um colégio jesuíta com René Descartes. Os dois estavam interessados em encontrar números perfeitos. Os números de Mersenne são construídos a partir de potências de 2, os números dobrados 2, 4, 8, 16, 32, 64, 128, 256, ..., e depois a subtração de um único 1. Um número de Mersenne é um número da forma  $2^n - 1$ . Embora eles sejam quase sempre ímpares, eles não são sempre primos. Mas são esses números de Mersenne que também são primos que podem ser usados para construir números perfeitos.

Mersenne sabia que, se a potência não fosse um número primo,



então o número de Mersenne tampouco podia ser um número primo, por causa das potências não primas 4, 6, 8, 9, 10, 12, 14 e 15 na tabela. Os números de Mersenne só poderiam ser primos se a potência fosse um número primo, mas será que isso bastava? Para os primeiros poucos casos, temos 3, 7, 31 e 127, que são todos primos. Então será geralmente verdadeiro que os números de Mersenne formados com uma potência prima deverão também ser primos?

Muitos matemáticos do mundo antigo até por volta do ano 1500 achavam que esse era o caso. Mas primos não são restritos pela simplicidade, e descobriu-se que para a potência 11 (um número primo),  $2^{11} - 1 = 2.047 = 23 \times 89$ . Consequentemente, este não é um número primo. Parecia não haver regra. Os números de Mersenne  $2^{17} - 1$  e  $2^{19} - 1$  são ambos primos, mas  $2^{23} - 1$  não é um primo, porque

$$2^{23} - 1 = 8.388.607 = 47 \times 178.481$$

## Apenas bons amigos

O matemático cabeça-dura em geral não é dado à mística de números, mas a numerologia ainda não está morta. Os números amigáveis vieram depois dos números perfeitos, embora talvez já fossem conhecidos pelos pitagóricos. Mais tarde se tornaram úteis na compilação de horóscopos românticos, onde suas propriedades matemáticas se traduziam na natureza da união etérea. Os dois números 220 e 284 são números amigáveis. Por quê? Bem, os divisores de 220 são 1, 2, 4, 5, 10, 11, 20, 22, 44, 55 e 110, e se você os somar, vai obter 284. E se calcular os divisores de 284 e os somar, adivinhe. Vai obter 220. Isso é amizade

verdadeira.

**Trabalho de construção** Uma combinação dos trabalhos de Euclides e de Euler dá uma fórmula que permite a geração de números perfeitos pares:  $n$  é um número perfeito par se e somente se  $n = 2^{p-1}(2^p - 1)$  onde  $2^p - 1$  é um primo de Mersenne.

## Os primos de Mersenne

Encontrar primos de Mersenne não é fácil. Muitos matemáticos ao longo dos séculos já fizeram acréscimos à lista, que tem uma história enigmática construída sobre uma combinação de erros e acertos. O grande Leonhard Euler contribuiu com o oitavo primo de Mersenne,  $2^{31} - 1 = 2.147.483.647$ , em 1732. Encontrar o 23º primo de Mersenne,  $2^{11213} - 1$ , em 1963, foi motivo de orgulho para o departamento de matemática da Universidade de Illinois, que o anunciou ao mundo no selo postal da universidade. Mas com computadores potentes a indústria dos primos de Mersenne foi adiante e, no final dos anos 1970, os estudantes Laura Nickel e Landon Noll, descobriram juntos o 25º primo de Mersenne. Até agora foram descobertos 45 primos de Mersenne.

Por exemplo,  $6 = 2^1(2^2 - 1)$ ,  $28 = 2^2(2^3 - 1)$  e  $496 = 2^4(2^5 - 1)$ . Essa fórmula para calcular números perfeitos pares significa que podemos gerá-los se conseguirmos encontrar primos de Mersenne. Os números perfeitos têm desafiado tanto pessoas como máquinas e vão continuar desafiando de um jeito que os matemáticos mais primitivos não tinham previsto. Ao escrever no início do século XIX, o elaborador de tabelas Peter Barlow

achou que ninguém iria além do cálculo do número perfeito de Euler

$$2^{30}(2^{31} - 1) = 2.305.843.008.139.952.128$$

já que não havia motivo para isso. Ele não conseguia prever a potência dos computadores modernos ou a necessidade insaciável dos matemáticos de enfrentar novos desafios.

**Números perfeitos ímpares** Ninguém sabe se um número perfeito ímpar será algum dia encontrado. Descartes achava que não, mas especialistas podem errar. O matemático inglês James Joseph Sylvester declarou que a existência de um número perfeito ímpar “seria praticamente um milagre” porque teria de satisfazer a muitas condições. Não é de surpreender que Sylvester fosse ambíguo. É um dos problemas mais antigos da matemática, mas se um número perfeito ímpar existir, muito já se sabe a seu respeito. Teria de ter pelo menos 8 diferentes divisores primos, um dos quais é maior do que um milhão, e ao mesmo tempo teria de ter pelo menos 300 algarismos.

**A ideia condensada:  
a mística dos números**

# 11 Números de Fibonacci

## linha do tempo

1202 d.C.	1724	1923	1963	2007
Leonardo de Pisa publica o <i>Liber Abaci</i> e os números de Fibonacci	Daniel Bernoulli expressa os números da sequência de Fibonacci em termos da proporção áurea	Bartók compõe a "Suite de dança", supostamente inspirada pelos números de Fibonacci	É fundado um periódico, o <i>Fibonacci Quarterly</i> , dedicado à teoria dos números da sequência de Fibonacci	O escultor Peter Randall-Page cria a escultura "Seed", de 70 toneladas, baseada na sequência de Fibonacci para o Eden Project na Cornualha, Reino Unido

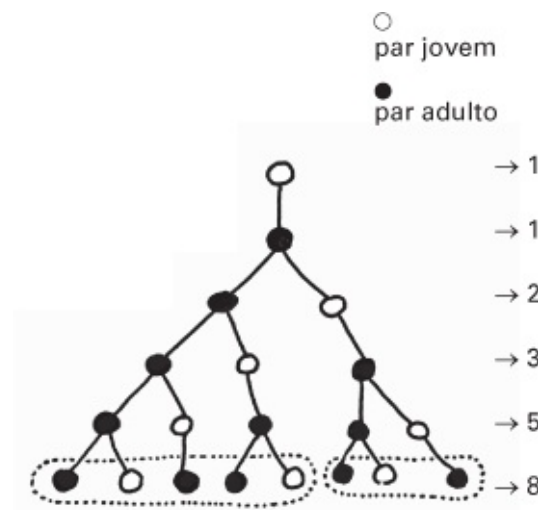
**Em *O código Da Vinci*, o autor Dan Brown fez com que seu curador assassinado, Jacques Saunière, deixasse os oito primeiros termos de uma sequência de números como pista sobre seu destino. Foram necessárias as habilidades da criptógrafa Sophie Neveu em reagrupar os números 13, 3, 2, 21, 1, 1, 8 e 5 para descobrir o que significavam. Bem-vindo à mais famosa sequência de números em toda a matemática.**

A sequência de números inteiros de Fibonacci é: 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, 1.597, 2.584,...

A sequência é bastante conhecida por suas muitas propriedades intrigantes. A mais básica – de fato, a feição característica que a define – é que cada termo é a soma dos dois anteriores. Por exemplo,  $8 = 5 + 3$ ,  $13 = 8 + 5$ , ...,  $2.584 = 1.587 + 987$ , e daí por diante. É só lembrar de começar com os dois números 1 e 1 e você consegue gerar o resto da sequência na hora. A sequência de Fibonacci é encontrada na natureza como o número de espirais formadas pelo número de sementes nas espirais dos girassóis (por exemplo, 34 em uma direção, 55 na outra), e usada por arquitetos nos projetos das proporções de salas e de construções. Os compositores de música clássica têm usado essa sequência como inspiração, e se acredita que a Suíte de Dança de Bartók está ligada à sequência. Na música contemporânea Brian

Transeau (também conhecido como BT) tem uma faixa em seu álbum *This Binary Universe* chamada 1,618 como saudação à suprema proporção dos números de Fibonacci, um número que vamos discutir um pouco mais adiante.

**Origens** A sequência de Fibonacci surgiu no *Liber Abaci*, publicado em 1202 por Leonardo de Pisa (Fibonacci), mas esses números já eram provavelmente conhecidos na Índia antes disso. Fibonacci apresentou o seguinte problema de geração de coelhos: *Pares de coelhos maduros geram pares de coelhos jovens a cada mês. No início do ano há um par jovem de coelhos. No final do primeiro mês eles terão amadurecido, e ao fim do segundo mês o par maduro ainda está lá e terão gerado um par de coelhos jovens. O processo de maturação e geração continua. Por algum milagre, nenhum dos pares de coelhos morre.*



Esquema da população de coelhos

Fibonacci queria saber quantos pares de coelhos haveria no fim do ano. As gerações podem ser mostradas em uma árvore genealógica. Vamos olhar o número de pares no fim de maio (o

quinto mês). Vemos que o número de pares é 8. Nessa camada da árvore genealógica o grupo da esquerda ●○●●○

é uma duplicata de toda a linha acima, e o grupo da direita ●○●

é uma duplicata da linha acima dela. Isso mostra que o nascimento de pares de coelhos segue a equação básica de Fibonacci: número depois de  $n$  meses = número depois de  $(n - 1)$  mês + número depois de  $(n - 2)$  meses.

**Propriedades** Vejamos o que acontece se somarmos os termos da sequência:  $1 + 1 = 2$

$$1 + 1 + 2 = 4$$

$$1 + 1 + 2 + 3 = 7$$

$$1 + 1 + 2 + 3 + 5 = 12$$

$$1 + 1 + 2 + 3 + 5 + 8 = 20$$

$$1 + 1 + 2 + 3 + 5 + 8 + 13 = 33$$

O resultado de cada uma dessas somas também vai formar uma sequência, que podemos arrumar sob a sequência original, mas

	Fibonacci	1	1	2	3	5	8	13	21	34	55	89...
com um desvio:	Soma	2	4	7	12	20	33	54	88...			

A soma dos  $n$  termos da sequência de Fibonacci acaba sendo 1 menor que a seguinte menos um número de Fibonacci. Se você quiser saber a resposta da soma  $1 + 1 + 2 + \dots + 987$ , basta subtrair um de 2.584 para obter 2.583. Se os números forem somados alternadamente, deixando-se termos de fora, como  $1 + 2 + 5 + 13 + 34$ , obtemos a resposta 55, ele próprio um número de Fibonacci. Se for adotada a outra alternativa, como  $1 + 3 + 8 + 21 + 55$ , a resposta é 88, que é um número de Fibonacci menos 1.

Os quadrados da sequência de números de Fibonacci também são

interessantes. Obtemos uma nova sequência multiplicando cada número de Fibonacci por ele mesmo e somando-os.

Fibonacci	1	1	2	3	5	8	<u>13</u>	<u>21</u>	34	55...
Quadrados	1	1	4	9	25	64	169	441	1.156	3.025...
Soma dos quadrados	1	2	6	15	40	104	<u>273</u>	714	1.870	4.895...

Nesse caso, somar todos os quadrados até o  $n$ -ésimo membro é a mesma coisa que multiplicar o  $n$ -ésimo membro da sequência de Fibonacci original pelo número seguinte a esse. Por exemplo,  $1 + 1 + 4 + 9 + 25 + 64 + 169 = 273 = 13 \times 21$

Os números de Fibonacci ocorrem também quando você menos espera. Vamos imaginar que tenhamos uma bolsa contendo uma mistura de moedas de £1 e de £2. Suponhamos que queremos contar o número de formas pelas quais as moedas podem ser retiradas da bolsa para totalizar uma quantia especial expressa em libras esterlinas. Nesse problema, a ordem das ações é importante. Ao tirarmos as moedas da bolsa, o valor £4 pode ser obtido por qualquer um dos seguintes modos,  $1 + 1 + 1 + 1$ ;  $2 + 1 + 1$ ;  $1 + 2 + 1$ ;  $1 + 1 + 2$  e  $2 + 2$ . No total são 5 modos, e isso corresponde ao quinto número de Fibonacci. Se você precisar de £20 há 6.765 modos de retirar moedas de £1 e £2, correspondendo ao 21º número de Fibonacci! Isso mostra o poder de ideias matemáticas simples.

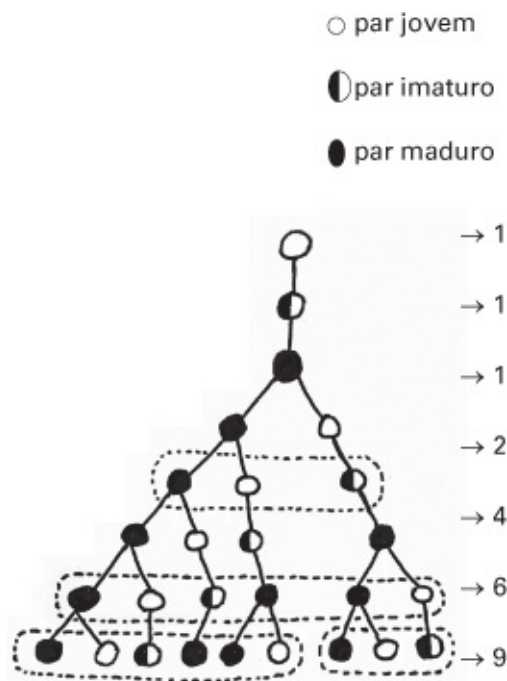
**A proporção áurea** Se olharmos para os termos formados com a sequência de Fibonacci, ao dividir um termo por seu precedente encontramos outra propriedade notável dos números de Fibonacci. Vamos fazer essa sequência para alguns poucos termos 1, 1, 2, 3, 5, 8, 13, 21, 34, 55.

1/1	2/1	3/2	5/3	8/5	13/8	21/13	34/21	55/34
1,000	2,000	1,500	1,333	1,600	1,625	1,615	1,619	1,617

Logo, as proporções se aproximam de um valor conhecido como a proporção áurea, um número famoso na matemática e designado pela letra grega  $\Phi$ . Esse número tem seu lugar entre as principais constantes matemáticas, como  $\pi$  e  $e$ , e tem o valor

exato de  $\phi = \frac{1+\sqrt{5}}{2}$

que pode ser uma aproximação do decimal 1,618033988... Com um pouco mais de trabalho podemos mostrar que cada número de Fibonacci pode ser escrito em termos de  $\Phi$ .



Esquema de população de bovinos

Apesar da quantidade de conhecimentos acumulados a respeito da sequência de Fibonacci, muitas questões ainda estão sem resposta. Os primeiros números primos na sequência de



Fibonacci são 2, 3, 5, 13, 89, 233, 1.597 – mas não sabemos se há uma infinidade de primos nela.

**Semelhanças de família** A sequência de Fibonacci tem um lugar privilegiado em uma família de sequências semelhantes de amplo espectro. Há um membro espetacular da família que podemos associar a um problema de população de bovinos. Em vez dos pares de coelhos de Fibonacci que se transformam em um mês de par jovem a par maduro, que então começa a se reproduzir, no caso do gado há um estágio intermediário no processo de maturação, quando os pares de bovinos progridem de pares jovens a pares imaturos, e daí para pares maduros. Só os pares maduros se reproduzem. A sequência de bovinos é: 1, 1, 1, 2, 3, 4, 6, 9, 13, 19, 28, 41, 60, 88, 129, 189, 277, 406, 595, ...

Então, a geração pula um valor, de modo que, por exemplo,  $41 = 28 + 13$  e  $60 = 41 + 19$ . Essa sequência tem propriedades semelhantes à sequência de Fibonacci. Para a sequência de bovinos, as proporções obtidas dividindo-se um termo por seu precedente aproximam-se do limite denotado pela letra grega psi, escrita  $\Psi$ , onde  $\Psi = 1,4655771233187676802665...$

que é conhecido como a “proporção superáurea”.

**A ideia condensada:  
o código Da Vinci  
decifrado**

# 12 Retângulos áureos

## linha do tempo

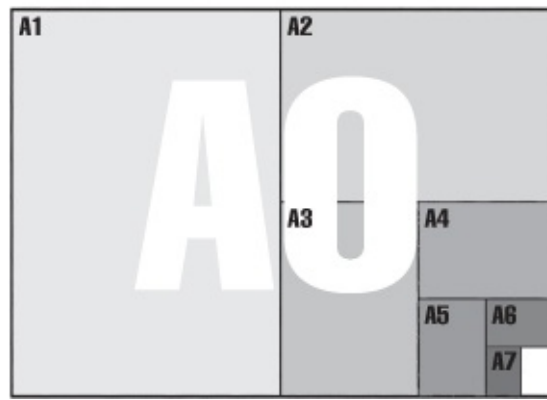
c.300 a.C.	1202 d.C.	1509	1876	1975
A razão extrema e média é publicada nos <i>Elementos</i> de Euclides	Leonardo de Pisa publica <i>Liber Abaci</i>	Pacioli publica <i>A proporção divina</i>	Fechner escreve sobre experiências psicológicas para determinar as proporções do retângulo "mais estético"	A Organização Internacional de Padronização (ISO) define o tamanho de papel A

**Os retângulos estão por toda parte – prédios, fotografias, janelas, portas, até este livro. Os retângulos estão presentes dentro da comunidade dos artistas – Piet Mondrian, Ben Nicholson e outros, que progrediram na direção da abstração, todos usaram um tipo ou outro de retângulo. Então qual é o mais bonito de todos? Será um “retângulo de Giacometti”, longo, fino, ou um retângulo que seja quase um quadrado? Ou será um retângulo entre esses dois extremos?**

Será que a pergunta sequer chega a fazer sentido? Alguns acham que sim, e acreditam que retângulos especiais são mais “ideais” do que outros. Desses, talvez o retângulo áureo seja o preferido. Entre todos os retângulos que se possam escolher por suas diversas proporções – por que é a isso que se resume a questão – o retângulo áureo é um retângulo muito especial, que já inspirou artistas, arquitetos e matemáticos. Olhemos primeiro para alguns outros retângulos.

**Papel matemático** Se pegarmos uma folha de papel A4, cujas dimensões são um lado curto de 210 mm e um lado longo de 297 mm, a razão entre comprimento e largura será de  $297/210$ , que é aproximadamente 1,4142. Para qualquer papel internacional de tamanho A com o lado curto igual a  $b$ , o lado longo será sempre

$1,4142 \times b$ . Então, o A4 tem  $b = 210$  mm, enquanto o A5 terá  $b = 148$  mm. O sistema do tamanho A usado para tamanhos de papel tem uma propriedade altamente desejável, que não ocorre em papéis de tamanhos arbitrários. Se uma folha de papel tamanho A é dobrada ao meio, os dois retângulos menores formados estão em uma razão direta com o retângulo maior. São duas versões menores do mesmo retângulo.




Dessa maneira, uma folha de papel A4 dobrada em dois gera duas folhas A5. Do mesmo modo, uma folha de A5 gera duas folhas de A6. Na outra direção, uma folha de papel A3 é feita de duas folhas de A4. Quanto menor o número no tamanho A, maior é a folha de papel. Como sabemos que esse número 1,4142 em especial iria fazer isso? Vamos dobrar um retângulo, mas dessa vez sem sabermos o comprimento de seu lado longo. Se tomamos a largura de um retângulo como sendo 1 e anotarmos o comprimento de seu lado longo como  $x$ , então a razão entre comprimento e largura é  $x/1$ . Se agora dobramos o retângulo, a razão entre comprimento e largura do retângulo menor será  $1 \div x/2$ , que é o mesmo que  $2/x$ . A questão a respeito dos tamanhos A é que nossas duas relações devem servir para a mesma

proporção, de modo que obtemos  $x/1 = 2/x$  ou  $x^2 = 2$ . O valor verdadeiro de  $x$ , portanto, é  $\sqrt{2}$ , que é aproximadamente 1,4142.

**Ouro matemático** O retângulo áureo é diferente, mas apenas *ligeiramente* diferente. Dessa vez, o retângulo é dobrado ao longo da linha RS no diagrama, de modo que os pontos *MRSQ* formam os ângulos de um *quadrado*.

A propriedade fundamental do retângulo áureo é que o retângulo restante, *RNPS*, é proporcional ao retângulo maior – o que sobra deveria ser uma minirréplica do retângulo grande.

Como antes, digamos que a largura  $MQ = MR$  do retângulo grande tem 1 unidade de comprimento, enquanto vamos anotar o comprimento do lado maior  $MN$  como  $x$ . A razão entre comprimento e largura é outra vez  $x/1$ . Dessa vez, a largura do retângulo menor *RNPS* é  $MN - MR$ , que é  $x-1$ , de modo que a razão comprimento/largura desse triângulo é  $1/(x-1)$ . Igualando as razões, obtemos a equação

$$\frac{x}{1} = \frac{1}{x-1}$$


que pode ser multiplicada para dar  $x(x-1)=1$  ou  $x^2 = x+1$ . Uma solução aproximada é 1,618. Podemos facilmente verificar isso. Se digitar 1,618 em uma calculadora e multiplicá-lo por ele

mesmo, você obtém 2,618, que é o mesmo que  $x + 1 = 2,618$ . Esse número é a famosa proporção áurea e é designada pela letra grega  $\Phi$ . Sua definição e aproximação é dada por

$$\phi = \frac{1+\sqrt{5}}{2} = 1,61803398874989484820 \dots$$

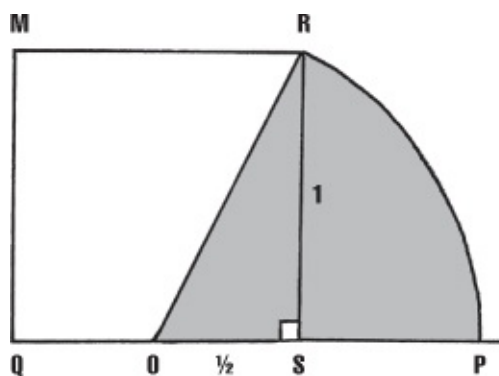
Esse número é relacionado à sequência de Fibonacci e ao problema do coelho (ver p. 47).

**Tentando o ouro** Agora vamos ver se conseguimos construir um retângulo áureo. Vamos começar com o nosso quadrado  $MQSR$  com lados iguais a 1 e marcar o meio  $QS$  como  $O$ . O comprimento  $OS = 1/2$ , então, pelo teorema de Pitágoras (ver p. 87), no triângulo  $ORS$ ,

$$OR = \sqrt{\left(\frac{1}{2}\right)^2 + 1^2} = \frac{\sqrt{5}}{2}$$

Usando um par de compassos centrados em  $O$  podemos desenhar o arco  $RP$  e vamos obter que  $OP = OR = \sqrt{5}/2$ . Então, acabamos tendo

$$QP = \frac{1}{2} + \frac{\sqrt{5}}{2} = \phi$$



Que é o que queríamos: a “seção áurea” ou o lado do retângulo

áureo.

**História** Exige-se muito da razão áurea  $\Phi$ . Uma vez percebidas as suas atraentes propriedades matemáticas, é possível vê-la em locais inesperados, até em lugares onde ela não está. Mais do que isso, é o perigo de se alegar que a razão áurea estava lá antes do artefato – que músicos, arquitetos e artistas estavam pensando nela no momento da criação. Esse ponto fraco é chamado de “numerismo áureo”. É um argumento perigoso passar dos números para declarações gerais sem outras provas.

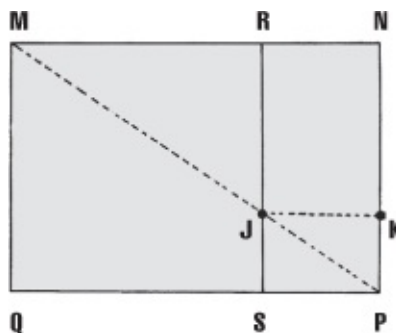
Considere o Partenon, em Atenas. Na época de sua construção a razão áurea era certamente conhecida, mas isso não significa que o Partenon tenha sido baseado nela. É claro, na fachada frontal do Partenon a razão da largura para a altura (incluindo o pendimento triangular) é de 1,74, que é próximo a 1,618, mas será que isso é próximo o suficiente para se reivindicar a proporção áurea como motivação? Algumas pessoas argumentam que o pendimento deveria ser deixado de fora do cálculo, e que se isso for feito, a razão entre a largura e a altura é na verdade o número inteiro 3.

Em seu livro *De divina proportione* de 1509, Luca Pacioli “descobriu” ligações entre características de Deus e propriedades da proporção determinada por  $\Phi$ . Batizou-a de “proporção divina”. Pacioli era um monge franciscano que escreveu influentes livros de matemática. Por alguns ele é visto como o “pai da contabilidade” porque popularizou o método de contabilidade chamado de entrada dupla usado pelos mercadores venezianos. Sua outra reivindicação à fama é que ele ensinou

matemática a Leonardo da Vinci. Na Renascença, a secção áurea alcançou um status quase místico – o astrônomo Johannes Kepler descreveu-a como uma “joia preciosa” da matemática. Mais tarde, Gustav Fechner, um psicólogo experimental alemão, fez milhares de medidas de formatos retangulares (cartas de jogar, livros, janelas) e descobriu que a razão de maior ocorrência entre seus lados era próxima a  $\Phi$ .

Le Corbusier era fascinado pelo retângulo como um elemento central no projeto de arquitetura e pelo retângulo áureo em particular. Ele colocava grande ênfase na harmonia e na ordem e encontrava isso na matemática. Via a arquitetura através dos olhos de um matemático. Uma de suas pranchas era o sistema “modulador”, uma teoria de proporções. Na verdade, esse era um jeito de gerar fluxos de retângulos áureos, feitos que ele usou em seus projetos. Le Corbusier foi inspirado por Leonardo da Vinci, que por sua vez tinha anotado cuidadosamente os trabalhos do arquiteto Romano Vitrúvio, o qual valorizava muito as proporções encontradas na figura humana.

**Outros formatos** Existe também um “retângulo superáureo”, cuja construção tem semelhanças com o modo pelo qual o retângulo áureo é construído.



É assim que criamos o retângulo superáureo  $MQPN$ . Como antes,  $MQSR$  é um quadrado cujo lado mede 1. Junte a diagonal  $MP$  e marque a interseção em  $RS$  como o ponto  $J$ . Em seguida, trace uma linha  $JK$ , paralela a  $RN$  com  $K$  em  $NP$ . Digamos que o comprimento  $RJ$  é  $y$  e que o comprimento  $MN$  é  $x$ . Para qualquer retângulo,  $RJ/MR = NP/MN$  (porque os triângulos  $MRJ$  e  $MNP$  são semelhantes), então  $y/1 = x/1$ , o que significa que  $x + y = 1$  e dizemos que  $x$  e  $y$  são recíprocas uma da outra. Obtemos o retângulo superáureo tornando o retângulo  $RJKN$  proporcional ao retângulo original  $MQPN$ , ou seja,  $y/(x - 1) = x/1$ . Usando o fato de que  $xy = 1$ , podemos concluir que o comprimento do retângulo superáureo  $x$  é encontrado resolvendo-se a equação “cúbica”  $x^3 = x^2 + 1$ , que é claramente semelhante à equação  $x^2 = x + 1$  (a equação que determina o retângulo áureo). A equação cúbica tem uma solução positiva real (substituindo  $x$  pelo símbolo mais padrão  $\Psi$ ), cujo valor é

$$\Psi = 1,46557123187676802665\dots,$$

que é o número associado com a sequência de bovinos (ver p. 49). Embora o retângulo áureo possa ser construído por uma beirada reta e um par de compassos, o retângulo superáureo não pode ser traçado desse jeito.

**A ideia condensada:  
proporções divinas**



# 13 Triângulo de Pascal

## linha do tempo

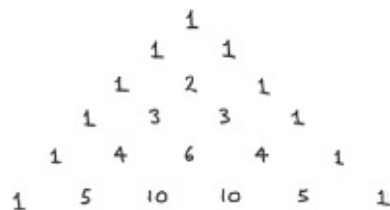
c.500 a.C.	c.1070 d.C.	1303	1664	1714
Evidências fragmentárias da existência do triângulo de Pascal em sânscrito	Omar Khayyam descobre o triângulo, que em alguns países tem o nome dele	Zhu Shijie define o triângulo de Pascal e mostra como somar determinadas sequências	O artigo de Pascal sobre as propriedades do triângulo é publicado postumamente.	Leibniz estuda o triângulo harmônico

O número 1 é importante. Mas e o 11? Também é interessante, e também  $11 \times 11 = 121$ ,  $11 \times 11 \times 11 = 1.331$  e  $11 \times 11 \times 11 \times 11 = 14.641$ . Arrumando tudo obtemos.

11  
121  
1331  
14.641  
15.101.051

Essas são as primeiras fileiras no triângulo de Pascal. Mas onde as encontramos?

Lançando no topo um  $11^0 = 1$  para garantir, a primeira coisa que fazemos é esquecer os pontos e depois introduzir espaços entre os números. Então, 14.641 passa a ser 1 4 6 4 1.

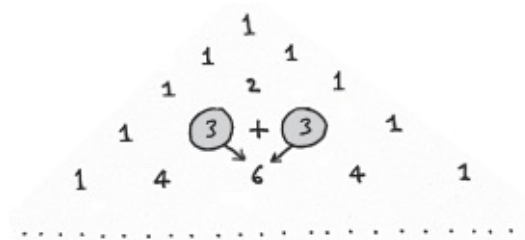


Triângulo de Pascal

O triângulo de Pascal é famoso na matemática por sua simetria e seus relacionamentos ocultos. Em 1653, Blaise Pascal descobriu isso e notou que seria impossível ele cobrir todos esses

relacionamentos em um artigo. As muitas ligações do triângulo de Pascal com outros ramos da matemática passaram a ser um objeto de estudo matemático venerável, mas suas origens remontam a muito antes disso. Na verdade, Pascal não inventou o triângulo que leva seu nome – já era conhecido dos estudiosos chineses do século XIII.

O padrão de Pascal é gerado a partir do topo. Comece com 1 e ponha dois 1s de cada lado dele na linha seguinte abaixo. Para construir mais linhas, continuamos a botar 1s nas extremidades de cada fileira enquanto os números internos são obtidos pela soma dos dois números imediatamente acima. Para obter 6 na quinta fila, por exemplo, somamos  $3 + 3$  da fileira acima.



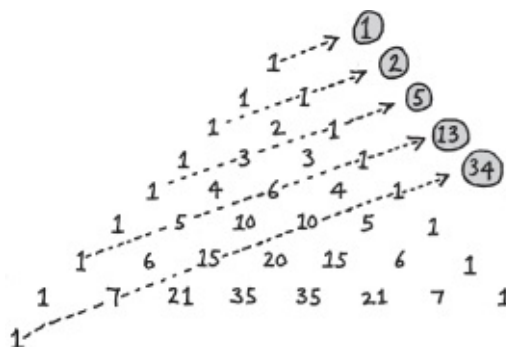
O matemático inglês G.H. Hardy disse que “um matemático, do mesmo modo que um pintor ou um poeta, é um fazedor de padrões” e o triângulo de Pascal tem padrões à beça.

**Ligações com a álgebra** O triângulo de Pascal é baseado em matemática de verdade. Se calcularmos  $(1 + x) \times (1 + x) \times (1 + x) = (1 + x)^3$ , por exemplo, obtemos  $1 + 3x + 3x^2 + x^3$ . Olhe atentamente e vai ver que os números na frente dos símbolos na expressão combinam com os números na fileira correspondente do triângulo de Pascal. O esquema seguido é:

$$\begin{array}{ccccccc}
 (1+x)^0 & & & & & & 1 \\
 (1+x)^1 & & & & 1 & 1 & \\
 (1+x)^2 & & & 1 & 2 & 1 & \\
 (1+x)^3 & & 1 & 3 & 3 & 1 & \\
 (1+x)^4 & 1 & 4 & 6 & 4 & 1 & \\
 (1+x)^5 & 1 & 5 & 10 & 10 & 5 & 1
 \end{array}$$

Se somarmos os números em qualquer fileira no triângulo de Pascal, obteremos sempre uma potência de 2. Por exemplo, na quinta fileira de baixo  $1 + 4 + 6 + 4 + 1 = 16 = 2^4$ . Podemos obter esse resultado a partir da coluna da esquerda acima se usarmos  $x = 1$ .

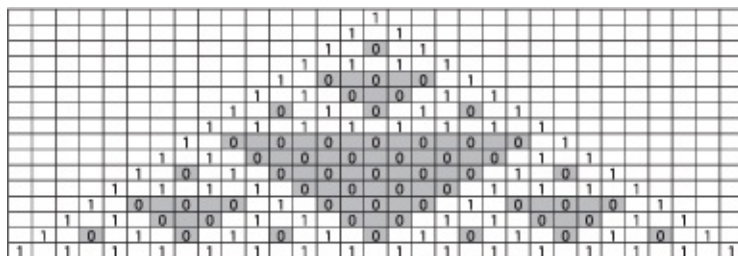
**Propriedades** A primeira e mais notável propriedade do triângulo de Pascal é sua simetria. Se desenharmos uma linha vertical através do meio, o triângulo tem “simetria especular” – o triângulo à esquerda da linha vertical é igual ao da direita da mesma linha. Isso permite que falemos a respeito de simples “diagonais”, porque uma diagonal para o nordeste será igual à diagonal para o noroeste. Sob a diagonal feita de 1s temos a diagonal feita dos números inteiros 1, 2, 3, 4, 5, 6,... Sob ela, temos os números triangulares 1, 3, 6, 10, 15, 21,... (os números que podem ser feitos de pontos sob a forma de triângulos). Na diagonal embaixo dela, temos os números tetraédricos 1, 4, 10, 20, 35, 56,... Esses números correspondem ao tetraedro (“triângulos tridimensionais” ou, se quiser, o números de balas de canhão que podem ser dispostas em bases triangulares de tamanhos crescentes). E que tal as “quase diagonais”?



Quase diagonais no triângulo de Pascal

Se somarmos os números em linhas através do triângulo (que não são linhas nem diagonais verdadeiras), obtemos a sequência 1, 2, 5, 13, 34,... Cada número é três vezes o número anterior subtraindo-se o que vem antes dele. Por exemplo,  $34 = 3 \times 13 - 5$ . Com base nisso, o número seguinte na sequência será  $3 \times 34 - 13 = 89$ . Perdemos a alternativa “quase diagonal”, começando com 1,  $1 + 2 = 3$ , mas esses nos darão a sequência 1, 3, 8, 21, 55... que são gerados pela mesma regra “3 vezes menos 1”. Podemos, desse jeito, gerar o próximo número na sequência como  $3 \times 55 - 21 = 144$ . Mas tem mais. Intercalando essas duas sequências de “quase diagonais” obtemos os números de Fibonacci:

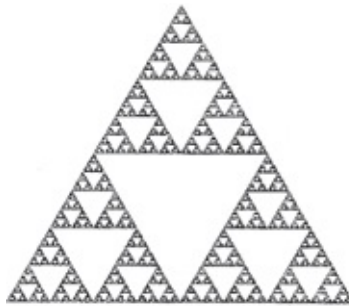
1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144...



Números pares e ímpares no triângulo de Pascal

**Combinações de Pascal** Os números de Pascal solucionam alguns problemas de contagem. Pense em 7 pessoas em uma sala.

Vamos chamá-las de Alison, Catherine, Emma, Gary, John, Matthew e Thomas. Quantos jeitos diferentes existem para escolher diferentes grupos de 3 entre eles? Um jeito seria A, C, E; outro seria A, C, T. Os matemáticos gostam de escrever  $C(n,r)$  para representar o número na  $n$ ésima linha na posição  $r$  (contando a partir de  $r = 0$ ) do triângulo de Pascal. A resposta para a nossa questão é  $C(7,3)$ . O número na 7ª linha do triângulo, na 3ª posição, é 35. Se escolhermos um grupo de 3 teremos automaticamente escolhido um grupo “não escolhido” de 4 pessoas. Isso se dá pelo fato de que  $C(7,4) = 35$  também. Em geral,  $C(n, r) = C(n, n - r)$ , que segue da simetria especular do triângulo de Pascal.



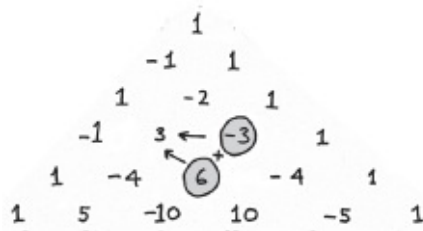
## A gaxeta de Sierpinski

**Os e 1s** No triângulo de Pascal, vemos que os números interiores formam um padrão, dependendo de se eles são pares ou ímpares. Se substituirmos 1 pelos números ímpares e 0 pelos números pares obtemos uma representação que mostra o mesmo padrão que o notável fractal conhecido como a gaxeta de Sierpinski (ver p. 104).

**Acrescentando sinais** Podemos anotar o triângulo de Pascal que corresponde às potências de  $(-1 \times x)$ , ou seja,  $(-1 + x)^n$ .

Nesse caso, o triângulo não é completamente simétrico em relação à linha vertical, e em vez de as somas das linhas resultarem em potências de 2, o resultado da soma é zero. Entretanto, as diagonais é que são interessantes aqui. A diagonal sudoeste 1, -1, 1, -1, 1, -1, 1, -1... são os coeficientes da expansão

$$(1 + x)^{-1} = 1 - x + x^2 - x^3 + x^4 - x^5 + x^6 - x^7 + \dots$$

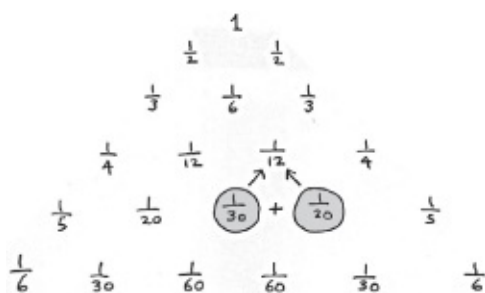


## Acrescentando sinais

Enquanto os termos na diagonal seguinte, ao longo, são os coeficientes da expansão

$$(1 + x)^{-2} = 1 - 2x + 3x^2 - 4x^3 + 5x^4 - 6x^5 + 7x^6 - 8x^7 + \dots$$

**O triângulo harmônico de Leibniz** O erudito alemão Gottfried Leibniz descobriu um notável conjunto de números sob a forma de um triângulo. Os números de Leibniz têm uma relação de simetria em torno da linha vertical. Mas diferentemente do triângulo de Pascal, o número em uma linha é obtido somando-se os dois números embaixo dele. Por exemplo,  $1/30 + 1/20 = 1/12$ . Para construir esse triângulo podemos avançar a partir do topo e andar da esquerda para a direita por subtração: conhecemos  $1/12$  e  $1/30$  e então  $1/12 - 1/30 = 1/20$ , o número ao lado de  $1/30$ . Você pode ter notado que a diagonal de fora é a famosa série harmônica



O triângulo harmônico de Leibniz

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \dots$$

Mas a segunda diagonal é que é conhecida como série de Leibniz,

$$\frac{1}{1 \times 2} + \frac{1}{2 \times 3} + \cdots + \frac{1}{n \times (n + 1)}$$

que por meio de manipulação inteligente acaba sendo igual a  $n/(n+1)$ . Exatamente como fizemos antes, podemos escrever esses números de Leibniz como  $B(n, r)$  para corresponder ao  $n$ ésimo número na linha  $r$ . Eles são relacionados aos números de Pascal  $C(n, r)$  pela fórmula:

$$B(n, r) \times C(n, r) = \frac{1}{n+1}$$

Como diz a velha canção, “o gato no rato, o rato na aranha, a aranha na velha e a velha a fiar”. Assim acontece com o triângulo de Pascal e suas ligações íntimas com tantas partes da matemática – geometria moderna, análise combinatória e álgebra, para citar apenas três. Mais do que isso, é um exemplo do intercâmbio matemático – a busca constante do padrão e da harmonia que reforça a nossa compreensão do assunto propriamente dito.

**A ideia condensada:  
a fonte de números**



# 14 Álgebra

## linha do tempo

1950 a.C.	250 d.C.	825	1591	Década de 1920	1930
Os babilônios trabalham com equações quadráticas	Diofanto de Alexandria publica <i>Aritmética</i>	Derivada de "al-jabr", Al-Khwarizmi lega a palavra "álgebra" à matemática	François Viète escreve um texto matemático em termos de letras para valores conhecidos e incógnitas	Emmy Noether publica artigos sobre o desenvolvimento da álgebra moderna abstrata	Bartel van der Waerden publica seu famoso <i>Moderne Algebra</i>

A álgebra nos fornece um modo distinto de resolver problemas, um método dedutivo com uma guinada. A guinada é “pensar o inverso”. Por um instante considere o problema de tomar o número 25, somar 17 a ele e obter 42. Isso é o pensamento em sentido direto. Nos são dados números e apenas os somamos. Mas e se, em vez disso, nos dessem a resposta 42 e nos fizessem uma pergunta diferente? Agora queremos saber o número que, ao ser somado a 25, nos dá 42. É aqui que entra o pensamento inverso. Queremos o valor de  $x$  que resolve a equação  $25 + x = 42$  e subtraímos 25 de 42 para obtê-lo.

Problemas com palavras a serem resolvidos por álgebra têm sido dados a estudantes há séculos:

*Minha sobrinha Michelle tem 6 anos e eu tenho 40. Quando terei três vezes a idade dela?*

Podemos encontrar isso pelo método da tentativa e erro, mas a álgebra é mais econômica. Em  $x$  anos a partir de agora Michelle terá  $6 + x$  anos e eu terei  $40 + x$ . Terei três vezes a idade dela quando

$$3 \times (6 + x) = 40 + x$$

Multiplique o lado esquerdo da equação e você vai obter  $18 + 3x = 40 + x$ , e passando os  $x$ s para um dos lados da equação e os números para o outro, encontramos que  $2x = 22$ , o que significa que  $x = 11$ . Quando eu tiver 51 anos Michelle terá 17. Mágica!

E se eu quisesse saber quando terei o dobro da idade dela? Podemos usar a mesma abordagem, dessa vez resolvendo

$$2 \times (6 + x) = 40 + x$$

para obter  $x = 28$ . Ela terá 34 quando eu tiver 68. Todas as equações acima são do tipo mais simples – são chamadas equações “lineares”. Elas não têm termos como  $x^2$  ou  $x^3$ , que tornam as equações mais difíceis de resolver. Equações com termos tipo  $x^2$  são chamadas equações “quadráticas” e as com termos como  $x^3$  são chamadas “cúbicas”. No passado,  $x^2$  era representado como um quadrado porque um quadrado tem quatro lados e se usava o termo quadrático;  $x^3$  era representado com um cubo.

A matemática passou por uma grande mudança, quando se passou da aritmética para a ciência dos símbolos, ou álgebra. O avanço dos números para as letras é um grande salto mental, mas o esforço vale a pena.

**Origens** A álgebra era um elemento significativo no trabalho de estudiosos islâmicos no século IX. Al-Khwarizmi escreveu um livro-texto de matemática que continha a palavra árabe *al-jabr*. Ao lidar com problemas práticos em termos de equações lineares e quadráticas, a “ciência das equações” de Al-Khwarizmi nos deu a palavra “álgebra”. Mais tarde Omar Khayyam ficou

famoso por escrever o *Rubaiyat* e os versos imortais (em tradução).

*Uma jarra de vinho, uma forma de pão –  
e tu ao meu lado cantando na natureza selvagem,*

mas em 1070, com 22 anos de idade, ele escreveu um livro sobre álgebra no qual investigava a solução de equações cúbicas.

## **A conexão italiana**

A teoria das equações cúbicas foi plenamente desenvolvida durante a Renascença. Infelizmente, ela resultou em um incidente quando a matemática nem sempre se comportava muito bem. Scipione Del Ferro encontrou a solução para as várias formas especializadas da equação cúbica e, ouvindo falar disso, Niccolò Fontana – apelidado “Tartaglia” ou “o gago” –, um professor de Veneza, publicou seus próprios resultados sobre álgebra, mas manteve secretos seus métodos.

Girolamo Cardano, de Milão, convenceu Tartaglia a contar a ele qual era o seu método, mas teve de jurar guardar segredo. O método vazou e criou-se uma rivalidade entre eles quando Tartaglia descobriu que seu trabalho tinha sido publicado no livro *Ars Magna*, de Cardano, em 1545.

A grande obra de Girolano Cardano sobre matemática, publicada em 1545, foi um divisor de águas na teoria das equações, porque continha uma grande quantidade de resultados para equações cúbicas e quárticas – essas envolvendo um termo do tipo  $x^4$ . Essa enxurrada de pesquisas mostrou que as equações quadráticas, cúbicas e quárticas podiam todas ser resolvidas por

fórmulas envolvendo apenas as operações  $+$ ,  $-$ ,  $\times$ ,  $\div$ ,  $\sqrt{\phantom{x}}$  (a última operação significa a  $q^{\text{a}}$  raiz). Por exemplo, a equação quadrática  $ax^2 + bx + c = 0$  pode ser resolvida usando a fórmula

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

Se você quiser resolver a equação  $x^2 - 3x + 2 = 0$  tudo o que tem de fazer é substituir os valores  $a = 1$ ,  $b = -3$  e  $c = 2$  na fórmula.

As fórmulas para se resolver equações cúbicas e quárticas são longas e difíceis de se manejar, mas certamente existem. O que intrigava os matemáticos era que eles não conseguiam produzir uma fórmula que tivesse aplicação geral a equações envolvendo  $x^5$ , as equações “quínticas”. O que haveria de tão especial na quinta potência?

Em 1826, Niels Abel, que morreu muito cedo, apresentou uma solução notável para esse enigma da equação quártica. Ele chegou mesmo a provar um conceito negativo, quase sempre uma tarefa mais difícil do que provar que alguma coisa pode ser feita. Abel provou que não poderia haver uma fórmula para resolver todas as equações quárticas e concluiu que qualquer pesquisa a mais para esse Santo Graal específico seria fútil. Ele convenceu o andar de cima dos matemáticos, mas a notícia demorou muito tempo para se espalhar pelo mundo matemático mais amplo. Alguns matemáticos se recusaram a aceitar o resultado, e ainda em meados do século XIX havia gente publicando obras alegando ter encontrado a fórmula que não existe.

**O mundo moderno** Durante 500 anos álgebra significou “a teoria das equações”, mas houve novos desenvolvimentos no século XIX. As pessoas se deram conta de que os símbolos na álgebra poderiam representar muito mais do que apenas números – poderiam representar “proposições”, e então a álgebra estaria relacionada ao estudo da lógica. Eles poderiam até representar objetos de dimensões mais altas, como os encontrados na álgebra matricial (ver p. 158). E, como muitos não matemáticos desconfiavam há tempos, podiam até não representar nada e ser apenas símbolos movimentados de acordo com determinadas regras (formais).

Um evento significativo na álgebra ocorreu em 1843, quando o irlandês William Rowan Hamilton descobriu os quaterniões. Hamilton estava buscando um sistema de símbolos que pudesse estender o complexo bidimensional dos números complexos para dimensões mais altas. Durante muitos anos ele tentou símbolos tridimensionais, mas não conseguiu chegar a nenhum sistema satisfatório. Quando ele descia de manhã para o café, seus filhos perguntavam “Então, papai, você consegue *multiplicar* trios?” e ele era constrangido a responder que só conseguia somá-los e subtraí-los.

O sucesso veio inesperadamente. A busca pelo tridimensional era um beco sem saída – ele deveria partir para os símbolos tetradimensionais. Esse raio de inspiração foi recebido enquanto caminhava com sua mulher ao longo do Canal Real até Dublin. Ficou extasiado com a sensação da descoberta. Sem hesitar, o vândalo de 38 anos, Astrônomo Real da Irlanda e Cavaleiro do Reino, entalhou as relações de definição na pedra em Brougham

Bridge – um ponto que é hoje assinalado com uma placa. Com a data gravada na cabeça, o assunto passou a ser a obsessão de Hamilton. Ele deu aulas sobre isso ano após ano e publicou dois grossos livros sobre sua “flutuação para oeste, o sonho místico do quatro”.

Uma peculiaridade dos quaterniões é que a ordem dos fatores em sua multiplicação é vitalmente importante, ao contrário das regras da aritmética comum. Em 1844, o linguista e matemático alemão Hermann Grassmann publicou um outro sistema algébrico com um pouco menos de drama. Desconsiderado na época, esse sistema acabou tendo longo alcance. Hoje, tanto os quaterniões como a álgebra de Grassmann têm aplicações em geometria, física e computação gráfica.

**O abstrato** No século XX o paradigma dominante da álgebra era o método axiomático. Esse método já tinha sido usado por Euclides como base para a geometria, mas só foi aplicado à álgebra em data comparativamente recente.

Emmy Noether foi a defensora do método abstrato. Nessa álgebra moderna, a ideia crucial é a do estudo da estrutura pela qual os exemplos individuais são subordinados à ideia abstrata geral. Se os exemplos individuais tiverem a mesma estrutura, mas talvez notações diferentes, eles são chamados isomórficos.

A estrutura algébrica mais fundamental é um grupo, e isso é definido por uma lista de axiomas (ver p. 161). Há estruturas com menos axiomas (como os grupoides, semigrupos e quase-grupos) e estruturas com mais axiomas (como anéis, corpos não comutativos, domínios integrais e campos). Todas essas

palavras novas foram importadas para a matemática no início do século XX, à medida que a álgebra se transformou em uma ciência abstrata, conhecida como “álgebra moderna”.

**A ideia condensada:  
solucionando o  
desconhecido**

# 15 Algoritmo de Euclides

## linha do tempo

c. 300 a.C.	c. 300 d.C.	810	1202	Anos 1970
O algoritmo de Euclides é publicado no Livro 7 dos <i>Elementos</i>	Sun Tzu descobre o teorema chinês do resto	Al-Khwarizmi dá a palavra "algoritmo" à matemática.	Fibonacci publica trabalho sobre congruências em <i>Liber Abaci</i>	O teorema chinês do resto é aplicado à criptografia de mensagens

**Al-Khwarizmi nos deu a palavra “álgebra”, mas foi o seu livro de aritmética do século IX que nos deu a palavra “algoritmo”. Cada vez mais citado, é um conceito útil tanto para matemáticos como para cientistas de computação. Mas o que é um algoritmo? Se pudermos responder isso, estaremos na trilha de entender o algoritmo de divisão de Euclides**

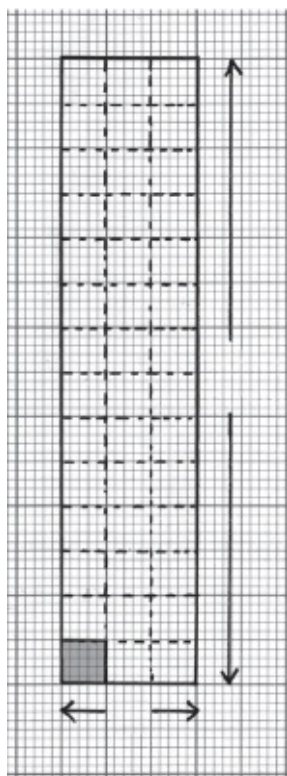
Em primeiro lugar, um algoritmo é uma rotina. É uma lista de instruções do tipo “faça isso e depois faça aquilo”. Dá para ver porque os computadores gostam de algoritmos, já que eles são muito bons em seguir instruções e nunca saem dos trilhos. Alguns matemáticos acham que os algoritmos são chatos porque são repetitivos, mas escrever um algoritmo e depois traduzi-lo em centenas de linhas de código computacional contendo instruções matemáticas não é coisa fácil. Há um risco considerável de dar tudo horivelmente errado. Escrever um algoritmo é um desafio criativo. Muitas vezes há diversos métodos disponíveis para executar a mesma tarefa e deve-se escolher o melhor. Alguns algoritmos podem não “servir para o objetivo” e outros podem ser francamente ineficientes porque não são diretos. Alguns podem ser rápidos, mas produzem a solução errada. É um pouco como cozinhar. Há provavelmente



centenas de receitas (algoritmos) para cozinhar um peru recheado. Certamente não queremos um algoritmo ruim para executar no único dia do ano em que isso importa. Então, temos os ingredientes e temos as instruções. O início da receita (abreviada) pode ser mais ou menos assim:

- Preencha a cavidade do peru com recheio
- Esfregue a pele exterior do peru com manteiga
- Tempere com sal, pimenta e páprica
- Asse a  $170^{\circ}\text{C}$  durante  $3\frac{1}{2}$  horas
- Deixe o peru assado descansar por  $\frac{1}{2}$  hora

É só seguir o algoritmo em passos sequenciais, um após o outro. A única coisa que está faltando nessa receita, algo em geral presente em um algoritmo matemático, é um *loop* (ciclo), uma ferramenta para lidar com a recorrência. Tomara que não tenhamos de assar o peru mais de uma vez.



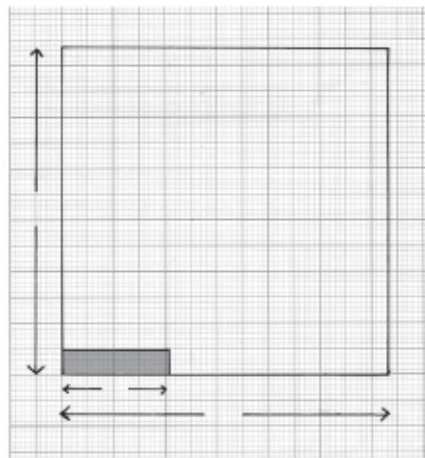
Ladrilhar um retângulo com um ladrilho quadrado  $6 \times 6$

Em matemática, também temos ingredientes – são os números. O algoritmo de divisão de Euclides é projetado para calcular o máximo divisor comum (escrito *mdc*). O *mdc* de dois números inteiros é o maior número que divide esses dois números. Como no exemplo dos ingredientes, vamos escolher os dois números 18 e 84.

**O máximo divisor comum** O *mdc* do nosso exemplo é o maior número que divide exatamente tanto 18 quanto 84. O número 2 divide tanto 18 quanto 84, mas o 3 também. Então, 6 também vai dividir os dois números. Será que há um número maior que os divida? Podemos tentar 9 ou 18. Ao verificarmos, esses candidatos não dividem 84, então o 6 é o maior número que divide os dois. Podemos concluir que o *mdc* de 18 e 84, escrito

como  $\text{mdc}(18, 84) = 6$ .

O  $\text{mdc}$  pode ser interpretado em termos de ladrilhos de cozinha. É o lado do maior ladrilho quadrado que vai cobrir uma parede retangular de 18 de largura e 84 de comprimento, sem ser permitido cortar ladrilhos. Nesse caso, podemos ver que o ladrilho de  $6 \times 6$  vai funcionar.



Ladrilhar o quadrado com um ladrilho retangular  $18 \times 84$

O máximo divisor comum é também conhecido como “o mais alto fator comum” ou “o mais alto divisor comum”. Existe também um conceito relacionado, o mínimo múltiplo comum ( $\text{mmc}$ ). O  $\text{mmc}$  de 18 e 84 é o menor número divisível tanto por 18 quanto por 84. A ligação entre  $\text{mmc}$  e  $\text{mdc}$  é enfatizada pelo fato de que o  $\text{mmc}$  de dois números multiplicados por seu  $\text{mdc}$  é igual à multiplicação dos dois números propriamente ditos. Aqui,  $\text{mmc}(18, 84) = 252$  e podemos verificar que  $6 \times 252 = 1512 = 18 \times 84$ .

Do ponto de vista da geometria, o  $\text{mmc}$  é o comprimento do lado do menor quadrado que possa ser coberto por ladrilhos retangulares de  $18 \times 84$ . Como  $\text{mmc}(a, b) = ab/\text{mdc}(a, b)$ , vamos

nos concentrar em encontrar o  $mdc$ . Já calculamos o  $mdc(18, 84) = 6$ , e para isso precisamos conhecer os divisores tanto de 18 como de 84.

Recapitulando, primeiro separamos os dois números em seus fatores:  $18 = 2 \times 3 \times 3$  e  $84 = 2 \times 3 \times 7$ . Depois, comparando-os, o número 2 é comum a ambos e é a mais alta potência de 2 que vai dividir os dois. Do mesmo modo, 3 é comum e é a maior potência que divide os dois, mas embora 7 divida 84, não divide 18, de modo que não pode entrar como fator no  $mdc$ . Concluimos que  $2 \times 3 = 6$  é o maior número que divide os dois. Será que esse jogo com os fatores pode ser evitado? Imagine os cálculos se quisermos encontrar o  $mdc(17.640, 54.054)$ . Vamos ter primeiro de fatorar esses dois números e isso seria apenas para começar. Tem de haver um modo mais simples.

**O algoritmo** Existe um modo melhor. O algoritmo de Euclides é dado no Livro 7 dos *Elementos*, Proposição 2 (na tradução): “Dados dois números não primos entre si, encontrar sua maior medida comum”.

O algoritmo de Euclides é lindamente eficiente e efetivamente substitui o esforço de encontrar fatores por simples substituição. Vejamos como funciona.

O objetivo é calcular  $d = mdc(18, 84)$ . Começamos por ver como 18 divide 84. Não divide exatamente, mas cabe 4 vezes, deixando 12 (o resto):

$$84 = 4 \times 18 + 12$$

Como  $d$  deve dividir tanto 84 quanto 18, deve também dividir o

resto, 12. Portanto,  $d = \text{mdc}(12, 18)$ . Então, agora podemos repetir o processo e dividir 18 por 12:

$$18 = 1 \times 12 + 6$$

para obter o resto 6, de modo que  $d = \text{mdc}(6, 12)$ . Ao dividir 12 em 6, temos o resultado 0, então  $d = \text{mdc}(0, 6)$ . Seis é o maior número que divide tanto 0 quanto 6, então essa é a nossa resposta.

Se computarmos  $d = \text{mdc}(17.640, 54.054)$ , os restos sucessivos serão 1.134, 630, 504 e 0, dando  $d = 126$ .

**Usos para o mdc** O *mdc* pode ser usado na solução de equações quando as soluções precisarem ser números inteiros. Elas são chamadas equações diofantinas, em homenagem ao antigo matemático grego Diofanto de Alexandria.

Imaginemos que a tia-avó Christine está indo para suas férias anuais em Barbados. Ela envia seu mordomo, John, para o aeroporto com sua coleção de malas, e cada uma delas pesa ou 18 kg ou 84 kg, e é informada de que o peso total registrado é de 652 kg. Ao chegar de volta a Belgravia, o filho de nove anos de John, James, diz “isso não pode estar certo porque o *mdc* 6 não divide 652”. James sugere que o peso total correto deve na verdade ser 642 kg.

James sabe que há uma solução em números inteiros para a equação  $18x + 84y = c$ , se e somente se o *mdc* 6 dividir o número  $c$ . Não funciona para  $c = 652$ , mas funciona para 642. James nem precisa saber quantas malas  $x, y$  de cada peso a tia Christine tem intenção de levar para Barbados.

**O teorema chinês do resto** Quando o  $\text{mdc}$  de dois números é 1 dizemos que eles são “relativamente primos”. Eles não têm de ser primos, eles mesmos, mas apenas têm de ser primos entre si, por exemplo  $\text{mdc}(6, 35) = 1$ , mesmo que nem 6 nem 35 sejam números primos. Vamos precisar disso para o teorema chinês do resto.

Olhemos para um outro problema: Angus não sabe quantas garrafas de vinho ele tem, mas quando as pareia, fica sobrando 1. Quando ele as põe em fileiras de cinco em sua prateleira de vinhos, sobram 3. Quantas garrafas ele tem? Sabemos que em divisão por 2 obtemos resto 1 e em divisão por 5 obtemos resto 2. A primeira condição permite que eliminemos todos os números pares. Repassando os números ímpares, rapidamente encontramos que o 13 serve (podemos em segurança supor que Angus tem mais do que 3 garrafas, um número que também satisfaz as condições). Mas há outros números que também poderiam estar corretos – na verdade uma sequência inteira começando com 13, 23, 33, 43, 53, 63, 73, 83...

Vamos agora acrescentar uma outra condição, de que o número deve deixar resto 3 em divisão por 7 (as garrafas chegaram em pacotes de 7, com 3 sobressalentes). Percorrendo a sequência 12, 23, 33, 43, 53, 63,... para levar isso em conta, percebemos que o 73 serve, mas notamos que o 143 também serve, e o 213 também, bem como qualquer número obtido pela soma de múltiplos de 70 a esses números.

Em termos matemáticos, encontramos soluções garantidas pelo teorema chinês do resto, que também diz que quaisquer duas

soluções diferem por um múltiplo de  $2 \times 5 \times 7 = 70$ . Se Angus tem entre 150 e 250 garrafas, então o teorema crava a solução em 213 garrafas. Nada mau para um teorema descoberto no século III.

## A ideia condensada:

**rota para o maior**



# 16 Lógica

## linha do tempo

c. 335 a.C.	1847 d.C.	1910	1965	1987
Aristóteles formaliza a lógica do silogismo	Boole publica <i>A análise matemática da lógica</i>	Russel e Whitehead tentam reduzir a matemática à lógica	Lofti Zadeh desenvolve a lógica difusa	O sistema de metrô no Japão é baseado na lógica difusa

**“Se houver menos carros nas estradas a poluição será aceitável. Ou temos menos carros na estrada ou deveria haver pedágio, ou as duas coisas. Se houver pedágio, o verão será insuportavelmente quente. O verão, na verdade, tem sido bastante fresco. Conclusão inescapável: a poluição é aceitável.”**

**Esse argumento, tirado do *lead* de um jornal diário é “válido” ou é ilógico? Não estamos interessados em se ele faz sentido do ponto de vista de política de trânsito rodoviário ou se é bom jornalismo. Estamos interessados apenas em sua validade como argumento racional. A lógica pode nos ajudar a decidir essa questão – já que diz respeito à rígida verificação do raciocínio.**

**Duas premissas e uma conclusão** Do jeito que está, a passagem do jornal é bastante complicada. Vamos primeiro olhar alguns argumentos mais simples, indo até o filósofo grego Aristóteles de Estagira, que é considerado o fundador da ciência da lógica. A abordagem dele usava diferentes formas de silogismos, um estilo de argumento com base em três declarações: duas premissas e uma conclusão. Um exemplo é

Todos os *spaniels* são  
cachorros  
Todos os cachorros são

animais

---

Todos os *spaniels* são animais

Acima da linha temos as premissas e abaixo dela, a conclusão. Nesse exemplo, a conclusão apresenta alguma inevitabilidade, não importa que significado liguemos às palavras “*spaniels*” e “animais”. O mesmo silogismo, mas usando palavras diferentes, é

Todas as maçãs são laranjas  
Todas as laranjas são bananas

---

Todas as maçãs são bananas

Neste caso, as declarações individuais são claramente sem sentido, se estivermos usando a conotação usual da palavra. No entanto, nos dois casos os silogismos têm a mesma estrutura e é a estrutura que torna o silogismo válido. É simplesmente impossível encontrar um exemplo de *As*, *Bs* e *Cs* com essa estrutura em que as premissas sejam verdadeiras, mas a conclusão seja falsa. É isso o que torna útil um argumento válido.

Todos os *As* são *Bs*  
Todos os *Bs* são *Cs*

---

Todos os *As* são *Cs*

Um argumento válido

É possível obtermos uma variedade de silogismo se variarmos os quantificadores como “todos”, “alguns”, “nenhum” (como nenhum *A* é *B*). Por exemplo, outro exemplo poderia ser

Alguns As são Bs  
Alguns Bs são Cs

---

Alguns As são Cs

Esse é um argumento válido? Será que se aplica a todos os casos de As, Bs e Cs, ou há algum contraexemplo à espreita, um caso em que as premissas são verdadeiras, mas a conclusão é falsa? E se chamarmos A de *spaniels*, B de objetos marrons e C de mesas? Será que o exemplo a seguir é convincente?

Alguns *spaniels* são marrons  
Alguns objetos marrons são  
mesas

---

Alguns *spaniels* são mesas

Nosso contraexemplo mostra que esse silogismo não é válido. Há tantos tipos diferentes de silogismos que estudiosos medievais inventaram um mnemônico para ajudar a lembrá-los. Nosso primeiro exemplo era conhecido como BARBARA porque contém três usos para “All” (“Todo”, *em inglês*). Esses métodos de análise de argumentos duraram mais de 2 mil anos e tiveram um lugar importante nos estudos de graduação nas universidades medievais. A lógica de Aristóteles – sua teoria do silogismo – foi considerada uma ciência perfeita até parte do século XIX.

**Lógica proposicional** Outro tipo de lógica vai além dos silogismos. Lida com as proposições, ou simples declarações, e com a combinação entre elas. Para analisar o *lead* do jornal, vamos precisar de algum conhecimento sobre essa “lógica proposicional”. Ela costumava ser chamada de “álgebra da

lógica”, o que nos dá um indício sobre sua estrutura, desde que George Boole se deu conta de que essa lógica podia ser tratada como um novo tipo de álgebra. Nos anos 1840 houve muito trabalho feito em lógica por matemáticos como Boole e Augustus De Morgan.

a	b	$a \vee b$
<b>V</b>	<b>V</b>	<b>V</b>
<b>V</b>	<b>F</b>	<b>V</b>
<b>F</b>	<b>V</b>	<b>V</b>
<b>F</b>	<b>F</b>	<b>F</b>

Tabela-verdade “ou”

Vamos experimentá-la e considerar a proposição **a**, onde **a** representa “Freddy é um *spaniel*”. A proposição **a** pode ser Verdadeira ou Falsa. Se estou pensando no meu cachorro chamado Freddy, que é mesmo um *spaniel*, então a declaração é verdadeira (**V**), mas se estou pensando que essa declaração está sendo aplicada ao meu primo cujo nome também é Freddy, então a declaração é falsa (**F**). A verdade ou falsidade de uma proposição depende de sua referência.

a	b	$a \wedge b$
<b>V</b>	<b>V</b>	<b>V</b>
<b>V</b>	<b>F</b>	<b>F</b>
<b>F</b>	<b>V</b>	<b>F</b>
<b>F</b>	<b>F</b>	<b>F</b>

Tabela-verdade “e”

Se tivermos outra proposição **b** tal como “Ethel é um gato”, então podemos combinar as duas proposições de várias maneiras. Uma combinação é escrita  $a \vee b$ . O conectivo  $\vee$  corresponde a “ou”, mas seu uso em lógica é ligeiramente diferente do “ou” na linguagem cotidiana. Em lógica  $a \vee b$  é verdadeira ou se “Freddy é um *spaniel*” é verdadeira ou se “Ethel é um gato” é verdadeira, ou se as duas forem verdadeiras, e só vai ser falsa se tanto **a** como **b** forem falsas. Essa conjunção de proposições pode ser resumida em uma tabela-verdade.

a	$\neg a$
<b>V</b>	<b>F</b>

<b>F</b>	<b>V</b>
----------	----------

Tabela-verdade “não”

Podemos também combinar proposições usando “e”, escrito como  $a \wedge b$ , e “não”, escrito como  $\neg a$ . A álgebra da lógica se torna clara quando combinamos essas proposições usando uma mistura de conectivos com **a**, **b** e **c** como  $a \wedge (b \vee c)$ . Podemos obter uma equação que chamamos de uma identidade:  $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$

a	b	$a \wedge b$
<b>V</b>	<b>V</b>	<b>V</b>
<b>V</b>	<b>F</b>	<b>F</b>
<b>F</b>	<b>V</b>	<b>V</b>
<b>F</b>	<b>F</b>	<b>V</b>

Tabela-verdade “implica”

O símbolo = significa equivalência entre as declarações lógicas,

onde os dois lados da equivalência têm a mesma tabela-verdade. Existe um paralelo entre a álgebra da lógica e a álgebra comum porque os símbolos  $\wedge$  e  $\vee$  funcionam de modo semelhante a  $\times$  e  $+$  na álgebra comum, onde temos  $x \times (y + z) = (x \times y) + (x \times z)$ . Entretanto, o paralelo não é exato e há exceções.

Outros conectivos lógicos podem ser definidos em termos desses básicos. Um conectivo útil é o conectivo de “implicação”  $a \rightarrow b$  que é definido como sendo equivalente a  $\neg a \vee b$  e tem a tabela-verdade mostrada.

Agora, se olharmos outra vez para o *lead* do jornal, podemos escrevê-lo na forma simbólica: **C** = menos **C** carros nas estradas  
**P** = a Poluição seria aceitável

$$C \rightarrow P$$

$$C \rightarrow E$$

$$E \rightarrow Q$$

$\neg Q$

---

**P**

**E** = deveria haver um **E** esquema de pedágio **Q** = o verão será insuportavelmente Quente Dando o argumento mostrado ao lado: Esse argumento é válido ou não? Vamos supor que a conclusão **P** é falsa, mas que todas as premissas são verdadeiras. Se pudermos mostrar que isso força uma contradição, significa que a conclusão é falsa. Se **P** é falso, então da primeira premissa,

$C \rightarrow P$ ,  $C$  deve ser falso. Como  $C \vee E$  é verdadeiro, o fato de que  $C$  é falso significa que  $E$  é verdadeiro. Dessa terceira premissa  $E \rightarrow Q$  significa que  $Q$  é verdadeiro. Ou seja,  $\neg Q$  é falso. Isso contradiz o fato de que  $\neg Q$ , a última premissa, era supostamente verdadeira. O conteúdo da declaração no *lead* do jornal ainda pode ser discutido, mas o argumento é válido.

**Outras lógicas** Gottlob Frege, C.S. Pierce e Ernst Schröder introduziram quantificação à lógica proposicional e construíram uma “lógica de predicados de primeira ordem” (porque suas variáveis podem ser quantificadas). Isso usa o quantificador universal  $\forall$ , para significar “para todo”, e o quantificador existencial,  $\exists$ , para significar “existe”.

Outro novo desenvolvimento na lógica é a ideia da lógica *fuzzy* (ou lógica difusa). Isso sugere pensamento confuso, mas na verdade é uma ampliação dos limites tradicionais da lógica. A lógica tradicional é baseada em coleções de conjuntos. Então, tivemos um conjunto de *spaniels*, o conjunto dos cachorros e o conjunto dos objetos marrons. Temos certeza do que está incluído no conjunto e do que não está incluído nele. Se encontrarmos um rodesiano puro sangue no parque, temos bastante certeza de que ele não é um membro do conjunto dos *spaniels*.

$\vee$

ou

e

$\wedge$

não

$\neg$



$\rightarrow$	implica
$\forall$	para todo
$\exists$	existe

A teoria dos conjuntos difusos lida com o que parecem ser conjuntos definidos sem precisão. E se tivéssemos o conjunto dos *spaniels* pesados? Que peso tem de ter um *spaniel* para ser incluído nesse conjunto? Com os conjuntos difusos há uma *gradação* na associação, e o contorno com respeito ao que está dentro e ao que está fora fica difuso. A matemática permite que sejamos precisos quanto à *fuzziness*. A lógica está longe de ser um assunto árido. Avançou, desde Aristóteles, e agora é uma área ativa de pesquisa moderna e aplicação.

**A ideia condensada:  
a linha clara do  
raciocínio**

# 17 Prova

## linha do tempo

c.300 a.C.	1637 d.C.	1838	1967	1976
Os <i>Elementos</i> de Euclides fornecem o modelo para a prova matemática	Descartes promove o rigor matemático como modelo em seu <i>Discurso sobre o método</i>	De Morgan introduz o termo "indução matemática"	Bishop prova resultados exclusivamente pelo método construtivo	Imre Lakatos publica o influente <i>Provas e refutações</i>

**Os matemáticos tentam justificar suas alegações por meio de provas. A busca de argumentos racionais rígidos é a força motriz da matemática pura. Cadeias de dedução corretas daquilo que é sabido ou é suposto levam o matemático a uma conclusão, que então entra para o depósito matemático estabelecido.**

Não se chega às provas facilmente – elas muitas vezes aparecem no final de muita exploração e trilhas falsas. A luta para chegar a elas ocupa o terreno central da vida do matemático. Uma prova bem-sucedida leva o selo de autenticidade do matemático, separando o teorema estabelecido da conjectura, ideia brilhante ou primeira suposição.

As qualidades buscadas em uma prova são rigor, transparência e, não menos, elegância. A isso acrescenta-se percepção. Uma boa prova é a que “nos torna mais sábios” – mas é também melhor ter alguma prova do que prova nenhuma. A progressão baseada em fatos não provados traz o perigo de que teorias possam ser construídas no equivalente matemático à base de areia.

Não que as provas durem para sempre, já que podem ter sido revistas à luz de desenvolvimentos nos conceitos com os quais elas se relacionam.

**O que é uma prova?** Quando lê ou ouve falar em um resultado matemático, você acredita nele? O que faria você acreditar? Uma resposta a essa pergunta seria um argumento lógico sólido, derivado de ideias que você aceita, até chegar à declaração sobre a qual você está se perguntando. Isso seria o que os matemáticos chamam de prova em sua forma comum, uma mistura da linguagem do dia a dia e da lógica rigorosa. Dependendo da qualidade da prova você ou se convence ou permanece cético.

Os principais tipos de provas empregados na matemática são: o método do contraexemplo; o método direto; o método indireto; e o método da indução matemática.

**O contraexemplo** Vamos começar sendo céticos – esse método visa provar que uma declaração é incorreta. Vamos tomar como exemplo uma declaração específica. Suponhamos que você ouve uma alegação de que qualquer número multiplicado por ele mesmo tem como resultado um número par. Você acredita nisso? Antes de partir para uma resposta devemos testar alguns exemplos. Se tivermos, digamos, o número 6 e o multiplicarmos por ele mesmo para obter  $6 \times 6 = 36$  descobrimos que 36 é realmente um número par. Mas uma andorinha só não faz verão. A alegação era para qualquer número e a quantidade deles é infinita. Para ter uma ideia do problema, deveríamos tentar mais alguns exemplos. Tentando 9, por exemplo, achamos que  $9 \times 9 = 81$ . Mas 81 é um número ímpar. Isso significa que a declaração de que *todos* os números, ao serem multiplicados por eles mesmos, resultem em um número par é falsa. Um exemplo desses vai contra a alegação original e é chamado de contraexemplo. Um contraexemplo à afirmação de que todos os

cisnes são brancos poderia ser ver um cisne negro. Parte da diversão na matemática é buscar um contraexemplo para derrubar um pretenso teorema.

Se não conseguimos encontrar um contraexemplo, podemos achar que a afirmativa é correta. Então, o matemático tem de fazer uma jogada diferente. Tem de construir uma prova, e o tipo mais direto é o método direto de prova.

**O método direto** No método direto, avançamos para a conclusão usando um argumento lógico a partir daquilo que já ficou estabelecido, ou que foi presumido. Se pudermos fazer isso, temos um teorema. Não conseguimos provar que se multiplicarmos qualquer número por ele mesmo o resultado é um número par, porque já refutamos essa afirmação. Mas talvez se salve alguma coisa. A diferença entre nosso primeiro exemplo, 6, e o contraexemplo, 9, é que o primeiro número é par e o contraexemplo é ímpar. Se mudarmos um pouco a hipótese, pode dar certo. Nossa nova afirmação é: multiplicando um número par por ele mesmo, o resultado é um número par.

Primeiro tentamos outros exemplos numéricos e descobrimos que essa afirmação é verificada todas as vezes e simplesmente não conseguimos achar um contraexemplo. Mudando de direção, tentamos provar isso, mas como podemos começar? Podíamos iniciar com um número geral  $n$ , mas como isso parece um tanto abstrato, vejamos como uma prova pode seguir, olhando para um número concreto, digamos 6. Como você sabe, um número par é um número que é múltiplo de 2, ou seja,  $6 = 2 \times 3$ . Como  $6 \times 6 = 6 + 6 + 6 + 6 + 6 + 6$  ou, escrito de outro jeito,  $6 \times 6 = 2 \times 3$

+  $2 \times 3 + 2 \times 3 + 2 \times 3 + 2 \times 3 + 2 \times 3$ , então, reescrevendo com parênteses,

$$6 \times 6 = 2 \times (3 + 3 + 3 + 3 + 3 + 3)$$

Isso significa que  $6 \times 6$  é um múltiplo de 2 e, como tal, é um número par. Mas nesse argumento não há nada que seja particular a 6, e poderíamos ter começado com  $n = 2 \times k$  para obter

$$n \times n = 2 \times (k + k + \dots + k)$$

e concluir que  $n \times n$  é par. Nossa prova agora está completa. Ao traduzir os *Elementos* de Euclides, os matemáticos mais modernos escreviam “CQD” no fim da prova para dizer que a tarefa tinha sido feita – é uma abreviação para “como queremos demonstrar”, em latim, “QED” (*quod erat demonstrandum*). Atualmente eles usam um quadrado cheio ■ (ou um quadrado vazio □). Isso é chamado de halmos em homenagem a Paul Halmos, que o introduziu.

**O método indireto** Nesse método, supomos que a conclusão é falsa e, por meio de um argumento lógico, demonstramos que isso contradiz a hipótese. Vamos provar o resultado anterior por esse método.

Nossa hipótese é de que  $n$  é par e vamos fingir que  $n \times n$  é ímpar. Podemos escrever  $n \times n = n + n + \dots + n$  e há  $n$  desses “enes”. Isso significa que  $n$  não pode ser par (porque se fosse,  $n \times n$  seria par). Então  $n$  é ímpar, o que contradiz a hipótese ■.

Isso é na verdade uma forma branda de método indireto. O

método indireto de força total é conhecido como o método do *reductio ad absurdum* (redução ao absurdo), e era muito estimado pelos gregos. Na academia em Atenas, Sócrates e Platão adoravam provar um ponto de debate envolvendo seus oponentes em um emaranhado de contradições e daí saía o ponto que eles estavam querendo provar. A prova clássica de que a raiz quadrada de 2 é um número irracional é desse formato, onde começamos supondo que a raiz quadrada de 2 é um número racional e derivamos uma contradição dessa suposição.

**O método da indução matemática** A indução matemática é um modo poderoso de demonstrar que uma sequência de afirmações  $P_1, P_2, P_3 \dots$  são todas verdadeiras. Isso foi reconhecido nos anos 1830 por Augustus De Morgan, que formalizou o que já se sabia há centenas de anos. Essa técnica específica (não confundir com indução científica) é amplamente usada para provar afirmações que envolvem números *inteiros*. É especialmente útil na teoria dos grafos, teoria dos números e ciência computacional em geral. Como exemplo prático, pense no problema de somar números ímpares. Por exemplo, a soma dos três primeiros números ímpares  $1 + 3 + 5$  é 9, enquanto a soma dos quatro primeiros,  $1 + 3 + 5 + 7$  é 16. Agora, 9 é  $3 \times 3 = 3^2$  e 16 é  $4 \times 4 = 4^2$ , então poderia a soma dos  $n$  primeiros números ímpares ser igual a  $n^2$ ? Se tentarmos um valor escolhido aleatoriamente de  $n$ , digamos  $n = 7$ , realmente perceberemos que a soma dos sete primeiros ímpares é  $1 + 3 + 5 + 7 + 9 + 11 + 13 = 49$ , que é  $7^2$ . Mas será que esse padrão é seguido por *todos* os valores de  $n$ ? Como poderemos ter certeza? Temos um problema, porque não podemos esperar verificar individualmente um número infinito

de casos.

É aí que entra a indução matemática. Informalmente, esse é o método de prova chamado dominó. Essa metáfora se aplica a uma fileira de dominós de pé. Se um dominó cai, ele derrubará o segundo. Isso é claro. Tudo o que precisamos para fazer com que *todos* caiam é derrubar o primeiro. Podemos aplicar esse pensamento ao problema dos números ímpares. A declaração  $P_n$  diz que a soma dos primeiros  $n$  números ímpares resulta em  $n^2$ . A indução matemática estabelece uma reação em cadeia pela qual  $P_1, P_2, P_3, \dots$  são todos verdadeiros. A afirmação  $P_1$  é trivialmente verdadeira porque  $1 = 1^2$ . Em seguida,  $P_2$  é verdadeira porque  $1 + 3 = 1^2 + 3 = 2^2$ ,  $P_3$  é verdadeiro porque  $1 + 3 + 5 = 2^2 + 5 = 3^2$  e  $P_4$  é verdadeiro porque  $1 + 3 + 5 + 7 = 3^2 + 7 = 4^2$ . Usamos o resultado como um estágio para pular para o seguinte. Esse processo pode ser formalizado para moldar o método da indução matemática.

**Dificuldades com a prova** As provas vêm sob todos os tipos de estilos e tamanhos. Algumas são curtas e intratáveis, especialmente aquelas encontradas em livros-texto. Algumas outras, que detalham a última pesquisa, preenchem edições inteiras de periódicos e chegam a milhares de páginas. Nesses casos, muito pouca gente vai conseguir perceber o argumento completo.

Há também questões fundamentais. Por exemplo, um número pequeno de matemáticos não aceita bem o método de prova indireta *reductio ad absurdum* quando se trata de existência. Se a suposição de que a solução de uma equação não existe levar a

uma contradição, será isso o suficiente para provar que existe uma solução? Oponentes desse método de prova vão alegar que a lógica não passa de um truque de prestidigitação e não nos diz como de fato construir uma solução concreta. Eles são chamados de “construtivistas” (de variadas matizes) que dizem que o método da prova não consegue prover “significado numérico”. Eles desprezam o matemático clássico que considera o método da redução ao absurdo uma arma essencial no arsenal matemático. Por outro lado, o matemático mais tradicional diria que proscrever esse tipo de argumento significa trabalhar com uma mão amarrada às costas, e além do mais, negar tantos resultados provados por esse método indireto deixa a tapeçaria dos matemáticos com uma aparência um tanto surrada.

## A ideia condensada:



**provado por A mais B**

# 18 Conjuntos

## linha do tempo

1872 d.C.	1881	1931	1939	1964
Cantor dá um passo hesitante na criação da teoria dos conjuntos	Venn populariza os “diagramas de Venn” para os conjuntos	Gödel prova que qualquer sistema matemático axiomático formal contém afirmações indecidíveis.	O pseudônimo Bourbaki é usado por matemáticos franceses	Cohen prova a independência da hipótese do <i>continuum</i>

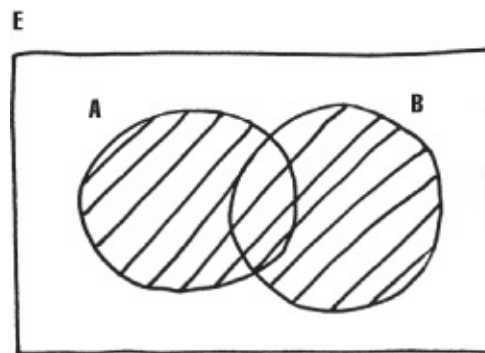
**Nicholas Bourbaki era o pseudônimo de um grupo autosselecionado de acadêmicos franceses que queriam reescrever a matemática de baixo para cima “do jeito certo”. A alegação arrojada deles era que a base de tudo deveria ser a teoria dos conjuntos. O método axiomático era fundamental e os livros que publicaram eram escritos no estilo rigoroso de “definição, teorema e prova”. Esse foi também o impulso do movimento da matemática moderna nos anos 1960.**

Georg Cantor criou a teoria dos conjuntos a partir de seu desejo de botar a teoria dos números reais em uma base sólida. Apesar das críticas e do preconceito iniciais, a teoria dos conjuntos ficou bem estabelecida como um ramo da matemática na virada do século XX.

**O que são conjuntos?** Um conjunto pode ser visto como uma coleção de objetos. Isso é informal, mas nos dá a ideia principal. Os objetos propriamente ditos são chamados de “elementos” ou “membros” do conjunto. Se escrevemos um conjunto  $A$  que tem um membro  $a$ , podemos escrever  $a \in A$ , como fez Cantor. Um exemplo é  $A = \{1, 2, 3, 4, 5\}$  e podemos escrever  $1 \in A$  para os que são membros e  $6 \notin A$  para os que não são membros.

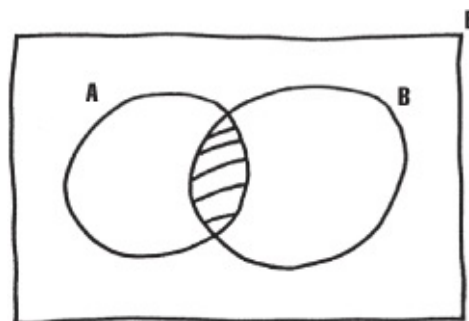
Os conjuntos podem ser combinados de modos interessantes. Se

$A$  e  $B$  são dois conjuntos, então o conjunto consistindo em elementos que são membros de  $A$  ou  $B$  (ou ambos) é chamado de “união de dois conjuntos”. Os matemáticos escrevem isso como  $A \cup B$ . Isso pode também ser descrito por um diagrama de Venn, que recebeu esse nome em homenagem ao lógico vitoriano, o reverendo John Venn. Euler usou diagramas como esse ainda mais cedo.



A união de  $A$  e  $B$

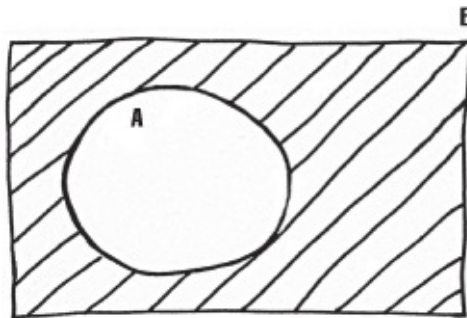
O conjunto  $A \cap B$  consiste em elementos que são membros de  $A$  e de  $B$  e é chamado de “interseção” dos dois conjuntos.



A intersecção de  $A$  e  $B$

Se  $A = \{1, 2, 3, 4, 5\}$  e  $B = \{1, 3, 5, 7, 10, 21\}$ , a união  $A \cup B = \{1, 2, 3, 4, 5, 7, 10, 21\}$  e a intersecção  $A \cap B = \{1, 3, 5\}$ . Se consideramos um conjunto  $A$  como fazendo parte de um conjunto universal  $E$ ,

podemos definir o conjunto complementar  $\neg A$  como consistindo nos elementos de  $E$  que não estão em  $A$ .



## O complemento de A

As operações  $\cap$  e  $\cup$  nos conjuntos são análogas a  $\times$  e  $+$  na álgebra. Com a operação complementar  $\neg$ , existe uma “álgebra dos conjuntos”. O matemático britânico nascido na Índia, Augustus De Morgan, formulou leis para mostrar como todas as três operações funcionam juntas. Na notação moderna, as leis De Morgan são:

$$\neg(A \cup B) = (\neg A) \cap (\neg B)$$

e

$$\neg(A \cap B) = (\neg A) \cup (\neg B)$$

**Os paradoxos** Não há problemas em lidar com conjuntos finitos porque podemos enumerar seus elementos, como em  $A = \{1, 2, 3, 4, 5\}$ , mas na época de Cantor os conjuntos infinitos eram mais desafiadores.

Cantor definiu os conjuntos como uma coleção de elementos dotados de uma propriedade específica. Pense no conjunto  $\{11, 12, 13, 14, 15, \dots\}$  todos números inteiros maiores do que 10. Como o conjunto é infinito não podemos anotar todos os seus elementos, mas ainda assim podemos especificá-lo pela propriedade que todos os seus membros têm em comum. Seguindo a indicação de Cantor, podemos escrever o conjunto como  $A = \{x: x \text{ é um número inteiro } > 10\}$ , onde os dois pontos significam “tal que”.

Na teoria primitiva dos conjuntos podíamos também ter um conjunto de coisas abstratas,  $A = \{x: x \text{ é uma coisa abstrata}\}$ . Nesse caso, o próprio  $A$  é uma coisa abstrata, de modo que é possível ter  $A \in A$ . Mas, ao permitir essa relação, surgem sérios problemas. O filósofo britânico Bertrand Russell apareceu com a ideia de um conjunto  $S$  que contém todas as coisas que não estão contidas nelas mesmas. Em símbolos, isso é  $S = \{x: x \notin x\}$

Ele depois fez a pergunta “será  $S \in S$ ?”. Se a resposta for “sim”, então  $S$  deverá satisfazer a sentença da definição para  $S$  e assim  $S \notin S$ . Por outro lado, se a resposta for “não” e  $S \notin S$ , então  $S$  satisfaz a relação definida de  $S = \{x: x \notin x\}$  e então  $S \in S$ . A questão

de Russel terminou com essa afirmação, que é a base do paradoxo de Russell.

$$S \in S \text{ se e somente se } S \notin S$$

Ele é semelhante ao “paradoxo do barbeiro”, em que um barbeiro da aldeia anuncia à população local que só fará a barba daqueles que não fazem a própria barba. Surge a questão: será que o barbeiro deve fazer a barba dele mesmo? Se ele não faz sua própria barba, deve se barbear. Se ele se barbeia, não deveria fazer sua própria barba.

Deve-se evitar tais paradoxos, educadamente chamados de “antinomias”. Para matemáticos simplesmente não é permissível ter sistemas que gerem contradições. Russell criou uma teoria de classes e só permitia  $a \in A$  se  $a$  pertencesse a uma classe inferior a  $A$ , desse modo evitando expressões tais como  $S \in S$ .

Outra maneira de evitar essas antinomias era formalizar a teoria dos conjuntos. Nessa abordagem, não nos preocupamos com a natureza dos conjuntos propriamente ditos, mas enumeramos axiomas formais que especificam regras para tratar com eles. Os gregos tentaram alguma coisa parecida com um problema deles mesmos – eles não tinham de explicar o que eram linhas retas, tinham apenas de explicar como deveriam lidar com elas.

No caso da teoria dos conjuntos, essa foi a origem dos axiomas de Zermelo–Fraenkel para a teoria dos conjuntos, que evitavam o aparecimento de conjuntos “grandes” demais em seu sistema. Isso de fato impedia que criaturas tão perigosas como o conjunto

de todos os conjuntos aparecessem.

**Teorema de Gödel** O matemático austríaco Kurt Gödel nocauteou aqueles que queriam fugir dos paradoxos com sistemas axiomáticos formais. Em 1931, Gödel provou que até para o sistema formal mais simples há afirmações cuja veracidade ou falsidade não poderiam ser deduzidos a partir desses sistemas. Em outras palavras, havia afirmações que estavam fora do alcance dos axiomas. Eram afirmações indecidíveis. Por esse motivo, o teorema de Gödel é parafraseado como o “teorema da incompletude”. Esse resultado se aplicava também ao sistema de Zermelo-Fraenkel, além de a outros sistemas.

**Números cardinais** É fácil contar o número de elementos de um conjunto finito; por exemplo,  $A = \{1, 2, 3, 4, 5\}$  tem 5 elementos, ou dizemos que sua “cardinalidade” é 5 e escrevemos  $\text{card}(A) = 5$ . Falando livremente, a cardinalidade mede o “tamanho” de um conjunto.

De acordo com a teoria dos conjuntos de Cantor, o conjunto de frações  $\mathbf{Q}$  e o dos números reais  $\mathbf{R}$  são muito diferentes. O conjunto  $\mathbf{Q}$  pode ser posto em uma lista, mas o conjunto  $\mathbf{R}$ , não (ver p. 32). Embora os dois conjuntos sejam infinitos, o conjunto  $\mathbf{R}$  tem uma ordem de infinitude maior do que  $\mathbf{Q}$ . Os matemáticos simbolizam  $\text{card}(\mathbf{Q})$  por  $\aleph_0$ , o “aleph zero” hebraico, e  $\text{card}(\mathbf{R}) = c$ . Isso significa  $\aleph_0 < c$ .

**A hipótese do continuum** Trazida à luz por Cantor em 1878, a hipótese do *continuum* diz que o nível seguinte de infinitude depois da infinitude de  $\mathbf{Q}$  é a infinitude dos números reais  $c$ . Dito de outro jeito, a hipótese do *continuum* determinou que não há



nenhum conjunto cuja cardinalidade esteja rigorosamente entre  $\aleph_0$  e  $c$ . A luta de Cantor era que, embora acreditasse que isso era verdade, não conseguia provar. Para provar o contrário ele teria de encontrar um subconjunto de  $\mathbf{R}$  com  $\aleph_0 < \text{card}(\xi) < c$ , o que ele também não conseguiu.

O problema era tão importante que o matemático alemão David Hilbert o colocou em primeiro lugar na sua famosa lista, apresentada no Congresso Internacional de Matemática em Paris em 1900, dos 23 problemas mais importantes para o século seguinte.

Gödel acreditara enfaticamente que a hipótese era falsa, mas não a provou. O que ele provou (em 1938) foi que a hipótese era compatível com os axiomas de Zermelo-Fraenkel para a teoria dos conjuntos. Um quarto de século mais tarde, Paul Cohen espantou Gödel e os lógicos provando que a hipótese do *continuum* não poderia ser deduzida a partir dos axiomas de Zermelo-Fraenkel. Isso equivale a mostrar que os axiomas e a negação da hipótese são consistentes. Combinado com o resultado de Gödel de 1938, Cohen tinha demonstrado que a hipótese do *continuum* era independente do resto dos axiomas da teoria dos conjuntos.

Esse estado de coisas é semelhante, em natureza, ao modo como o postulado do paralelo em geometria (ver p. 114) é independente dos demais axiomas de Euclides. Essa descoberta resultou em um florescimento de geometrias não euclidianas que, entre outras coisas, tornou possível o avanço da teoria da relatividade por Einstein. De modo semelhante, a hipótese do

*continuum* pode ser aceita ou rejeitada sem perturbar os demais axiomas da teoria dos conjuntos. Depois do resultado pioneiro de Cohen foi criado todo um novo campo, que atraiu gerações de matemáticos que adotaram as técnicas usadas por ele para provar a independência da hipótese do *continuum*.

**A ideia condensada:  
muitos tratados  
como um**

# 19 Cálculo

## linha do tempo

c. 450 d.C.	1660-1670 d.C.	1734	Década de 1820	1854	1902
Zenão ridicula os infinitesimais com um paradoxo	Newton e Leibniz dão os primeiros passos no Cálculo	Berkeley chama a atenção para as debilidades dos fundamentos	Cauchy formaliza a teoria de modo rigoroso	Riemann introduz a integral de Riemann	Lebesgue estabelece a teoria da integral de Lebesgue

**Um cálculo é uma maneira de calcular, de modo que os matemáticos algumas vezes falam a respeito de “cálculo da lógica”, de “cálculo da probabilidade” e daí por diante. Mas todos nós concordamos que só há realmente um Cálculo, puro e simples, e que é escrito com C maiúsculo.**

O Cálculo é uma plataforma central da matemática. Hoje em dia vai ser raro encontrar um cientista, engenheiro ou economista quantitativo que não tenha se deparado com o Cálculo, tão amplas são suas aplicações. Historicamente, está associado a Isaac Newton e Gottfried Leibniz, que foram os pioneiros do Cálculo no século XVII. Suas teorias semelhantes resultaram em uma disputa de prioridade sobre quem descobriu o Cálculo. Na verdade, os dois homens chegaram às suas conclusões de modo independente e seus métodos são bem diferentes.

Desde então o Cálculo se tornou um assunto enorme. Toda geração determina técnicas que acha que devem ser aprendidas pela geração mais jovem, e hoje em dia os livros-texto ultrapassam um milhar de páginas e envolvem muitos extras. Apesar de todos esses acréscimos, a diferenciação e a integração são absolutamente essenciais, os picos gêmeos do Cálculo como estabelecido por Newton e Leibniz. As palavras são derivadas do

*differentialis* de Leibniz (tomar as diferenças ou “partir”) e *integralis* (a soma das partes, ou “juntar”).

Na linguagem técnica, a diferenciação trata de medir *mudança*, e a integração de medir área, mas a joia da coroa do Cálculo é o “resultado relevante” de que há dois lados na mesma moeda – diferenciação e integração são os inversos uma da outra. O Cálculo, na verdade, é um assunto só e você precisa conhecer os dois lados. Não é de surpreender que o “*very model of a modern Major General*” [eu sou o próprio modelo de um major-general moderno] de Gilber e Sullivan na canção “Pirates of Penzance” orgulhosamente declarou os dois:

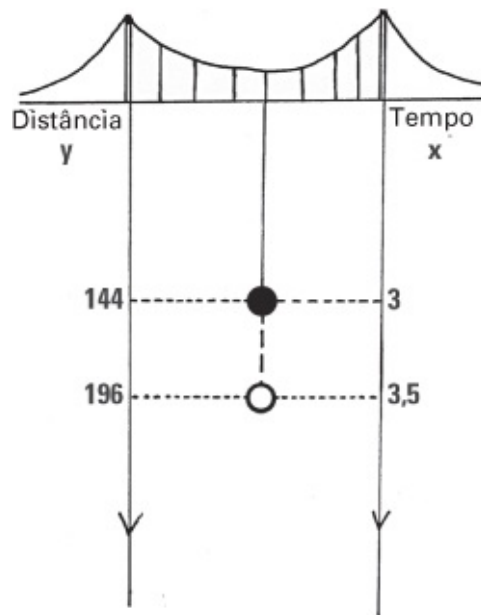
*With many cheerful facts about the square of the hypotenuse.  
I'm very good at integral and differential calculus.*<sup>[1]</sup>

**Diferenciação** Os cientistas gostam de comandar “experiências mentais” – Einstein gostava especialmente delas. Imagine que estamos de pé em cima de uma ponte bem acima de uma garganta e estamos a pique de deixar cair uma pedra. O que vai acontecer? A vantagem da experiência mental é que nós não temos de estar verdadeiramente lá, em pessoa. Podemos também fazer coisas impossíveis, como parar a pedra no meio da queda ou observá-la em movimento lento durante um curto intervalo de tempo.

De acordo com a teoria da gravidade de Newton, a pedra vai cair. Nada de surpreendente nisso; a pedra é atraída pela terra e vai cair cada vez mais depressa, enquanto o ponteiro do nosso cronômetro avança. Outra vantagem de uma experiência mental é que podemos deixar de lado fatores complicadores, como a

resistência do ar.

Qual é a velocidade da pedra em um dado instante de tempo, digamos, quando o cronômetro marca exatamente 3 segundos depois de a pedra ter sido largada? Como podemos calcular isso? Podemos certamente medir a velocidade *média*, mas nosso problema é medir a velocidade *instantânea*. Como é uma experiência mental, porque não paramos a pedra no meio da queda e depois a deixamos cair uma distância curta durante mais uma fração de segundo? Se dividirmos essa distância extra pelo tempo extra, vamos ter a velocidade média durante um curto intervalo de tempo. Adotando intervalos de tempo cada vez menores, a velocidade média vai ser cada vez mais próxima da velocidade instantânea no lugar onde fizemos a pedra parar. Esse processo de limitação é a ideia básica por trás do Cálculo.



Podemos ficar tentados a tornar o pequeno tempo a mais igual a zero. Mas na nossa experiência mental, a pedra não se moveu. Não andou distância alguma e não gastou tempo algum para

isso! Isso nos daria a velocidade média de 0/0, que o filósofo irlandês Bishop Berkeley descreveu muito bem como “os fantasmas das quantidades finadas” (“*ghosts of departed quantities*”). Essa expressão não pode ser determinada – na verdade ela não tem sentido. Mas, se adotarmos esse caminho, vamos acabar num atoleiro numérico.

Para prosseguir, precisamos de símbolos. A fórmula exata que liga a distância caída  $y$  e o tempo  $x$  levado para chegar lá foi derivada por Galileu:

$$y = 5 \times x^2$$

O fator “5” aparece porque as unidades de medida escolhidas foram metros e segundos. Se quisermos saber, digamos, quanto a pedra caiu em 3 segundos, simplesmente substituímos  $x = 3$  na fórmula e calculamos a resposta  $y = 5 \times 3^2 = 45$  metros. Mas como podemos calcular a *velocidade* da pedra em um tempo  $x = 3$ ?

Vamos tomar mais 0,5 de um segundo e ver que distância a mais a pedra percorreu entre 3 e 3,5 segundos. Em 3,5 segundos a pedra percorreu  $y = 5 \times 3,5^2 = 61,25$  metros, então entre 3 e 0,5 segundos ela caiu  $61,25 - 45 = 16,25$  metros. Como a velocidade é a distância dividida pelo tempo, a velocidade média durante esse intervalo de tempo é  $16,25/0,5 = 32,5$  metros por segundo. Isso seria próximo à velocidade instantânea em  $x = 3$ , mas você pode muito bem dizer que 0,5 não é uma medida suficientemente pequena. Repita o argumento com um menor intervalo de tempo, digamos 0,05 s, e veremos que a distância caída é  $46,51 - 45 = 1,51$  metro, dando uma velocidade média de

$1,51/0,05 = 30,25$  metros por segundo. Isso realmente será mais próximo à velocidade instantânea da pedra a 3 segundos (quando  $x=3$ ).

Agora teremos de pegar o touro pelos chifres e abordar o problema de calcular a velocidade média da pedra entre  $x$  segundos e ligeiramente mais tarde a  $x + h$  segundos. Depois de embaralhar um pouco os símbolos encontramos que isso é

$$5 \times (2x) + 5 \times h$$

À medida que fazemos com que  $h$  fique cada vez menor, como fizemos indo de 0,5 para 0,05, vemos que o primeiro termo não é afetado (porque não envolve  $h$ ) e o segundo se torna, ele mesmo, cada vez menor. Concluimos que

$$v = 5 \times (2x)$$

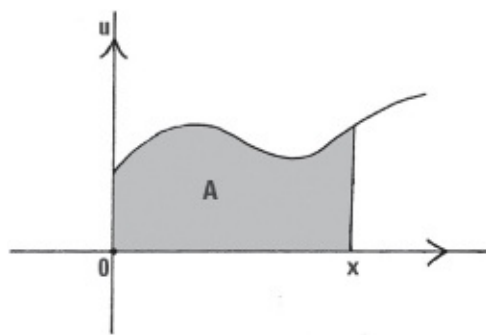
Onde  $v$  é a velocidade instantânea da pedra no tempo  $x$ . Por exemplo, a velocidade instantânea da pedra depois de 1 seg (quando  $x = 1$ ), é  $5 \times (2 \times 1) = 10$  metros por segundo; depois de 3 segundos é  $5 \times (2 \times 3)$ , o que dá 30 metros por segundo.

$u$	$du/dx$
$x^2$	$2x$
$x^3$	$3x^2$
$x^4$	$4x^3$
$x^5$	$5x^4$
...	...

$$x^n$$

$$nx^{n-1}$$

Se compararmos a fórmula da distância de Galileu  $y = 5 \times x^2$  com a fórmula da velocidade  $v = 5 \times (2x)$  a diferença essencial é a mudança de  $x^2$  para  $2x$ . Esse é o efeito da diferenciação, passando por  $u = x^2$  para a derivação  $\dot{u} = 2x$ . Newton chamou  $\dot{u} = 2x$  de uma “fluxão” e a variável  $x$  de fluente porque ele pensou nela em termos de quantidades que fluem. Hoje em dia nós frequentemente escrevemos  $u = x^2$ , e seus derivados como  $du/dx = 2x$ . Originalmente introduzida por Leibniz, o uso continuado dessa notação representa o sucesso do “d” ismo de Leibniz sobre os pontos de Newton”.



A pedra em queda foi um exemplo, mas se tivéssemos outras expressões representadas por  $u$  ainda poderíamos calcular a derivada, que pode ser útil em outros contextos. Há um padrão nisso: a derivada é formada pela multiplicação da potência anterior e subtraindo 1 dela para formar a nova potência.

**Integração** A primeira aplicação da integração foi medir superfície. A medida da área sob uma curva é feita dividindo-a em tiras aproximadamente retangulares, cada uma com largura  $dx$ . Medindo-se a área de cada uma e somando-as teremos a “soma”, portanto, a área total. A notação  $S$  significando soma



foi introduzida por Leibniz em uma forma alongada  $\int$ . A área de cada uma das tiras retangulares é  $u dx$ , de modo que a área  $A$  sob a curva de 0 a  $x$  é

$$A = \int_0^x u \, dx$$

Se estivermos examinando a curva  $u = x^2$ , a área é encontrada desenhando-se tiras retangulares estreitas sob a curva, somando-as para calcular a área aproximada, e aplicando o processo de limitação a suas larguras para obter a área exata. Essa resposta dá a área

$$A = x^3/3$$

$u$	$\int_0^x u \, dx$
$x^2$	$x^3/3$
$x^3$	$x^4/4$
$x^4$	$x^5/5$
$x^5$	$x^6/6$
...	...
$x^n$	$x^{n+1}/(n+1)$

Para diferentes curvas (portanto, para outras expressões de  $u$ ) podemos ainda calcular a integral. Do mesmo modo que na derivada, há um padrão regular para a integral de potências de  $x$ . A integral é formada dividindo-se a “potência anterior +1” e somando 1 a ela para formar a nova potência.

**O resultado relevante** Se diferenciarmos a integral  $A = x^3/3$  vamos realmente obter o original  $u = x^2$ . Se integrarmos a derivada  $du/dx = 2x$  também vamos obter o original  $u = x^2$ . A diferenciação é o inverso da integração, uma observação

conhecida como o Teorema Fundamental do Cálculo, e um dos teoremas mais importantes de toda matemática.

Sem o Cálculo não haveria satélites em órbita, não haveria teoria econômica e a estatística seria uma disciplina muito diferente. Onde houver mudança envolvida, encontramos o Cálculo.

**A ideia condensada:  
indo até o limite**

## 20 Construtos

### linha do tempo

450 a.C.	1672 d.C.	1801	1837	1882
Anaxágoras tenta fazer a quadratura do círculo enquanto estava na prisão	Mohr mostra que todos os construtos euclidianos podem ser feitos só com compasso	Gauss publica o <i>Discurso sobre a Aritmética</i> incluindo uma seção sobre a construção de um polígono regular de 17 lados com régua e compassos	Wantzel prova que os problemas clássicos de duplicar um cubo e trissecar um ângulo não podem ser resolvidos com régua e compasso	Lindemann prova que não se pode fazer a quadratura do círculo

**Provar uma negativa é muitas vezes difícil, mas alguns dos grandes triunfos da matemática fazem exatamente isso. Isso significa provar que alguma coisa não pode ser feita. A quadratura do círculo é impossível, mas como podemos provar?**

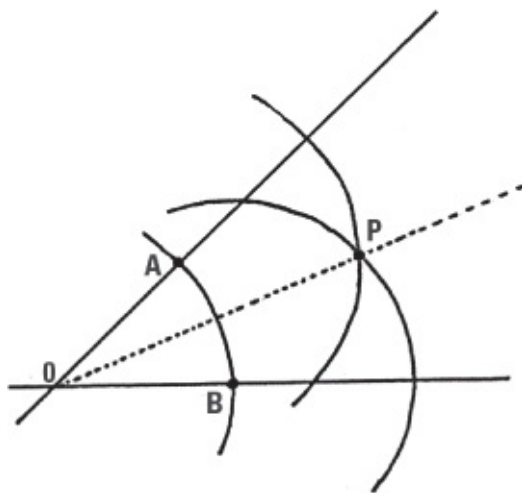
Os gregos antigos tinham quatro grandes problemas de construção:

- A trissecção de um triângulo (dividir um ângulo em três ângulos iguais menores).
- Dobrar o cubo (construir um segundo cubo com duas vezes o volume do primeiro).
- Quadratura do círculo (criar um quadrado com a mesma área de um determinado círculo).
- Construir polígonos (construir formatos regulares com lados e ângulos iguais).

Para executar essas tarefas, eles usavam apenas o mínimo necessário:

- Uma beirada reta, uma régua, para traçar linhas retas (e definitivamente *não* para medir comprimentos).
- Um par de compassos para desenhar círculos.

Se você gosta de escalar montanhas sem cordas, oxigênio, telefones celulares e outra parafernália, não há dúvida de que você vai gostar desses problemas. Sem equipamentos modernos de medição, as técnicas matemáticas necessárias para provar esses resultados eram sofisticadas, e os clássicos problemas de construção da antiguidade só foram solucionados no século XIX usando-se as técnicas de análise moderna e de álgebra abstrata.



Bissecção de um ângulo

**Bissecção e trissecção do triângulo** Aqui está um modo de dividir um ângulo em dois ângulos iguais menores ou, em outras palavras bissectá-lo. Primeiro, coloque a ponta do compasso em  $O$  e, com qualquer raio, marque  $AO$  e  $OB$ . Passando a ponta do compasso para  $A$ , trace um arco de círculo. Faça a mesma coisa em  $B$ . Marque o ponto de intersecção desses círculos  $P$ , e com a régua junte  $O$  a  $P$ . Os triângulos  $AOP$  e  $BOP$  serão idênticos no formato, portanto, os ângulos  $A\hat{O}P$  e  $B\hat{O}P$  serão iguais. A linha  $OP$  é a bissetriz exigida, dividindo o ângulo em dois ângulos iguais.

Será que podemos usar uma sequência de ações como essas para

dividir um ângulo arbitrário em três ângulos iguais? Esse é o problema da trissecção do ângulo.

Se o ângulo tiver  $90^\circ$ , um ângulo reto, não há problema, porque pode-se construir o ângulo de  $30^\circ$ . Mas se tomarmos o ângulo de  $60^\circ$ , por exemplo, esse ângulo não pode ser trissecado. Sabemos que a resposta é  $20^\circ$ , mas não há como construir esse ângulo usando apenas uma régua e compassos. Então, resumindo:

- Você pode *sempre* bissectar *todos* os ângulos
- Você pode *sempre* trissecar *alguns* ângulos, mas
- Há *alguns* ângulos que você *nunca* pode trissecar.

A duplicação do cubo é um problema semelhante, conhecido como o problema deliano. A história conta que os nativos de Delos, na Grécia, consultaram o oráculo por causa de uma praga que os estava castigando. Disseram a eles que construíssem um novo altar, com duas vezes o volume do já existente.

Imagine que o altar deliano começou como um cubo tridimensional com todos os lados com comprimentos iguais, digamos  $a$ . Então, eles precisavam construir outro cubo de comprimento  $b$  com o dobro do volume. O volume de cada um é  $a^3$  e  $b^3$  e eles são relacionados por  $b^3 = 2a^3$ , ou  $b = \sqrt[3]{2} \times a$  onde  $\sqrt[3]{2}$  é o número que multiplicado por ele mesmo três vezes dá 2 (a raiz cúbica). Se o lado do cubo original é  $a = 1$ , os habitantes de Delos tinham de marcar o comprimento em uma linha. Infelizmente para eles, isso é impossível com uma régua e compassos, não importa quanta engenhosidade eles aplicassem à construção futura.

**Quadratura do círculo** Esse problema é um pouco diferente e é o mais famoso dos problemas de construção:

*Construir um quadrado cuja área é igual à área de um dado círculo.*



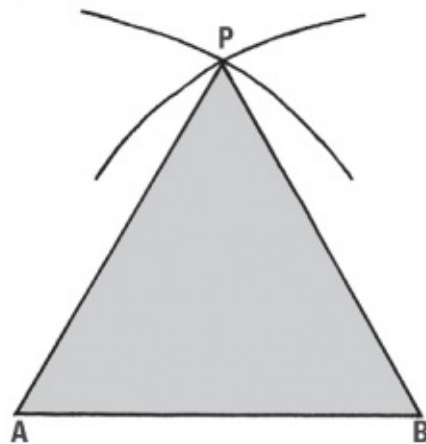
A quadratura do círculo

A expressão “quadratura do círculo” é comumente usada para expressar o impossível. A equação algébrica  $x^2 - 2 = 0$  tem soluções específicas  $x = \sqrt{2}$  e  $x = -\sqrt{2}$ . Esses são números irracionais (não podem ser escritos como frações), mas demonstrar que não se pode tornar o círculo quadrado significa provar que  $\pi$  não pode ser a solução para *qualquer* equação algébrica. Números irracionais com essa propriedade são chamados de números transcendentais porque eles têm uma irracionalidade “mais alta” do que seus parentes irracionais, como  $\sqrt{2}$ .

Em geral, os matemáticos acreditavam que  $\pi$  era um transcendental, mas esse “enigma das eras” era difícil de provar, até que Ferdinand von Lindemann usou uma modificação na técnica, usada pela primeira vez por Charles Hermite. Hermite já a tinha usado para lidar com um problema menos importante, provar que a base de logaritmos naturais,  $e$ , era transcendental (ver p. 28).

Seguindo o resultado de Lindemann, podemos pensar que a enxurrada de artigos produzida pelo bando indômito dos “quadradores de círculos” iria parar. Nem um pouco. Ainda dançando nas vias secundárias da matemática, havia aqueles relutantes em aceitar a lógica da prova, e alguns nunca nem ouviram falar nela.

**Construção de polígonos** Euclides apresentou o problema de como construir um polígono regular. Um polígono é uma figura simétrica dotada de vários lados, como um quadrado ou um pentágono, em que os lados têm comprimento igual e onde os lados adjacentes formam ângulos iguais uns com os outros. Em sua famosa obra *Elementos* (Livro 4), Euclides mostrou como os polígonos com 3, 4, 5 e 6 lados podiam ser construídos usando apenas nossas duas ferramentas básicas.



Construção de um triângulo equilátero

O polígono com 3 lados é o que normalmente chamamos de um triângulo equilátero e sua construção é particularmente direta. Não importa que comprimento você queira para o seu triângulo, chame uma ponta de A e outra de B, com a distância desejada

entre elas. Ponha a ponta do compasso em  $A$  e trace um arco do círculo de raio  $AB$ . Repita isso com a ponta do compasso em  $B$ , usando o mesmo raio. O ponto de intersecção desses dois arcos é em  $P$ . Como  $AP = AB$  e  $BP = AB$ , todos os lados do triângulo  $APB$  são iguais. O triângulo propriamente dito é completado unindo  $AB$ ,  $AP$  e  $BP$  usando a régua.

Se acha que ter uma régua é um luxo, você não está sozinho – o dinamarquês Georg Mohr também achava isso. O triângulo equilátero é construído achando-se o ponto  $P$ , e para isso só é preciso os compassos – a régua só era usada para unir *fisicamente* os pontos. Mohr mostrou que qualquer construto que possa ser elaborado com régua e compasso pode ser elaborado só com compasso. O italiano Lorenzo Mascheroni provou os mesmos resultados 125 anos mais tarde. Uma novidade em seu livro de 1797, *Geometria del Compasso*, dedicado a Napoleão, é que ele o escreveu em verso. Em relação ao problema geral, os polígonos com  $p$  lados, onde  $p$  é um número primo são especialmente importantes. Já construímos o polígono de 3 lados, e Euclides construiu o polígono de 5 lados, mas ele não conseguiu construir o polígono de 7 lados (o heptágono). Ao investigar esse problema aos 17 anos de idade, um certo Carl Friedrich Gauss provou uma negativa. Ele deduziu que não é possível construir um polígono de  $p$  lados para  $p = 7, 11$  ou  $13$ .

## Um príncipe nasceu

Carl Friedrich Gauss ficou tão impressionado com seu resultado mostrando que um polígono de 17 lados podia ser construído que ele resolveu botar de lado seu planejado estudo de línguas e se tornar



matemático. O resto é história – e ele ficou conhecido como “o príncipe dos matemáticos”. O polígono de 17 lados é o formato da base de seu memorial em Gotinga, na Alemanha, e é um tributo adequado ao seu gênio.

Mas Gauss provou também um positivo e concluiu que é possível construir um polígono com 17 lados. Gauss, na verdade, foi mais longe e provou que um polígono de  $p$  lados pode ser construído se, e somente se, o número primo  $p$  for da forma

$$p = 2^{2^n} + 1$$

Números dessa forma são chamados números de Fermat. Se os avaliarmos para  $n = 0, 1, 2, 3$  e  $4$ , vamos ver que são os números primos  $p = 3, 5, 17, 257$  e  $65.537$ , e que esses correspondem a polígonos que podem ser construídos, com  $p$  lados.

Quando tentamos  $n = 5$ , o número de Fermat é  $p = 2^{32} + 1 = 4.294.967.297$ . Pierre de Fermat conjecturou que eles eram todos números primos, mas infelizmente esse não é um número primo, porque  $4.294.967.297 = 641 \times 6.700.417$ . Se pusermos  $n = 6$  ou  $7$  na fórmula o resultado são enormes números de Fermat, mas com  $n = 5$ , nenhum dos dois é primo.

Será que há outros primos de Fermat? O que se diz até agora é que não, mas ninguém sabe ao certo..

## A ideia condensada:

**tome uma régua e um  
par de compassos...**

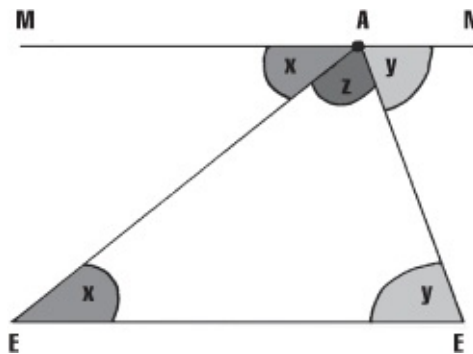
# 21 Triângulos

## linha do tempo

1850 a.C.	1335 d.C.	1571	1822	1873
Os babilônios conhecem o "teorema de Pitágoras"	Richard de Wallingford escreve um tratado inovador sobre trigonometria	François Viète publica um livro sobre trigonometria e tabelas trigonométricas	Karl Feuerbach descreve o círculo de nove pontos de um triângulo	Brocard produz seu exaustivo trabalho sobre o triângulo

O fato mais evidente a respeito de um triângulo é ele ser uma figura com três lados e três ângulos (triângulos). Trigonometria é a teoria que usamos para “medir o triângulo”, seja o tamanho dos ângulos, o comprimento dos lados ou a área contida dentro dele. Seu feitio – uma das figuras mais simples – é de interesse permanente.

**A história do triângulo** Há um argumento nítido para mostrar que os ângulos de qualquer triângulo somam dois ângulos retos, ou  $180^\circ$ . A partir do ponto do “vértice”  $A$  de qualquer triângulo, trace uma linha  $MAN$  paralela à base  $BC$ .



O ângulo  $\hat{ABC}$ , que vamos chamar de  $x$ , é igual ao ângulo  $\hat{BAM}$ , porque eles são ângulos alternos e  $MN$  e  $BC$  são paralelas. Os dois outros ângulos alternos são iguais a  $y$ . O ângulo em torno do ponto  $A$  é igual a  $180^\circ$  (metade de  $360^\circ$ ) e isso é  $x + y + z$ , que é a

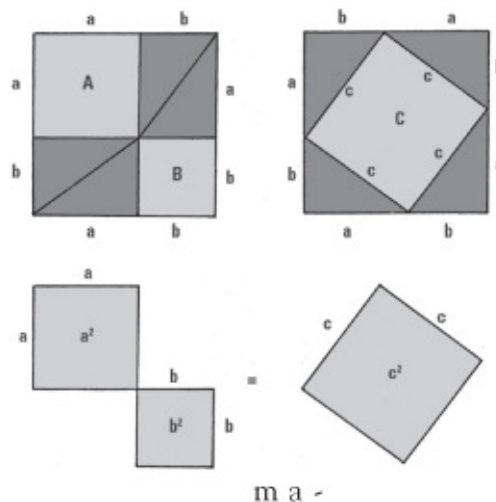
soma dos ângulos no triângulo. CQD, como era muitas vezes escrito no fim dessas provas. É claro que estamos supondo que o triângulo foi traçado em uma superfície plana, como essa folha plana de papel. Os ângulos de um triângulo traçado em uma bola (um triângulo esférico) não somam  $180^\circ$ , mas isso é outra história.

Euclides provou muitos teoremas a respeito de triângulos, sempre se certificando de que isso fosse feito pelo método dedutivo. Ele mostrou, por exemplo, que “em qualquer triângulo, dois lados tomados juntos de qualquer maneira são maiores do que o lado restante”. Hoje em dia isso é chamado a “desigualdade do triângulo” e tem importância em matemática abstrata. Os epicuristas, com sua abordagem pé-no-chão da vida, alegaram que isso não precisava de prova, porque era evidente até para um asno. Se um fardo de feno fosse posto no vértice de um triângulo e o asno no outro, argumentavam eles, o animal dificilmente passaria pelos dois lados para satisfazer a fome.

**Teorema de Pitágoras** O maior teorema de triângulo de todos é o teorema de Pitágoras, que aparece na matemática moderna – embora haja alguma dúvida se foi mesmo Pitágoras o primeiro a descobri-lo. A afirmativa mais conhecida é em termos de álgebra,  $a^2 + b^2 = c^2$ , mas Euclides na verdade se refere a formatos quadrados: “Em triângulos retângulos o quadrado do lado que subtende o ângulo reto é igual aos quadrados dos lados que contêm o ângulo reto”.

A prova de Euclides é a Proposição 47 no Livro 1 dos *Elementos*,

uma prova que se tornou um ponto de ansiedade para gerações de alunos quando eles tinham de pelejar para decorá-la ou aguentar as consequências. Há centenas de provas em existência. Uma favorita é mais no espírito de Bhaskara, do século XII, do que uma prova euclidiana de 300 a.C.



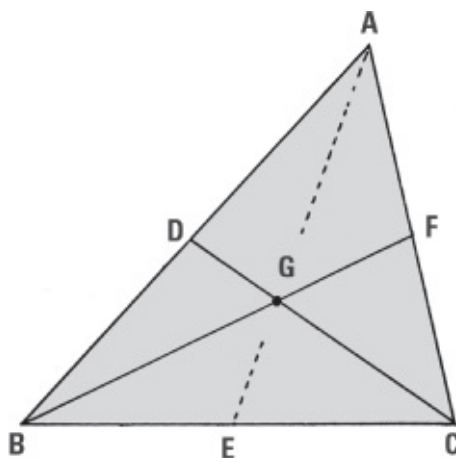
Essa é uma “prova sem palavras”. Na figura, o quadrado com lado  $a + b$  pode ser dividido de dois modos diferentes.

Como os quatro triângulos iguais (sombreados em escuro) são comuns a ambos os quadrados, podemos retirá-los e ainda continuar com a mesma área. Se olharmos para as áreas dos formatos re-manescentes, aparece a conhecida expressão

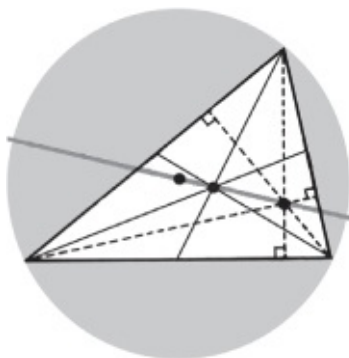
$$a^2 + b^2 = c^2$$

**A linha de Euler** É possível ter centenas de proposições sobre triângulos. Primeiro, vamos pensar a respeito dos pontos médios dos lados. Em qualquer triângulo  $ABC$  marcamos os pontos médios  $D, E, F$  de seus lados. Junte  $B$  a  $F$  e  $C$  a  $D$  e marque o ponto onde elas cruzam  $G$ . Agora una  $A$  a  $E$ . Será que essa linha

também passa através de  $G$ ? Não é evidente que ela deva necessariamente passar através de  $G$  sem avançar no raciocínio. De fato, passa, e o ponto  $G$  é chamado de “centroide” do triângulo. Esse é o centro de gravidade do triângulo.



Há literalmente centenas de diferentes “centros” ligados a um triângulo. Outro é o ponto  $H$ , onde as alturas (linhas perpendiculares a uma base traçadas a partir de um vértice – mostrado por linhas pontilhadas na figura da p. 87) se encontram. Esse é chamado de “ortocentro”. Há também outro centro chamado de “circuncentro”  $O$ , em que cada uma das linhas (conhecidas como “perpendiculares”, não mostradas) em  $D$ ,  $E$  e  $F$  se encontram. Esse é o centro do círculo que pode ser traçado por  $A$ ,  $B$  e  $C$ .



## Linha de Euler

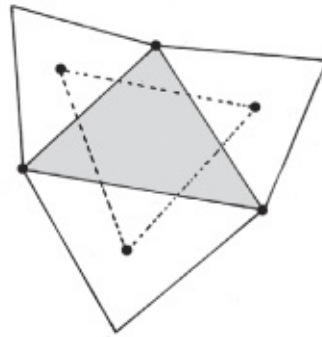
Mas há mais verdades. Em qualquer triângulo  $ABC$  os centros  $G$ ,  $H$  e  $O$ , respectivamente, o centroide, o ortocentro e o circuncentro, se localizam ao longo de uma linha, chamada “linha de Euler”. No caso de um triângulo equilátero (todos os lados têm o mesmo comprimento), esses três pontos coincidem e o ponto resultante é inequivocamente o centro do triângulo.

**Teorema de Napoleão** Para qualquer triângulo  $ABC$ , triângulos equiláteros podem ser construídos sobre cada lado, e a partir de seus centros constrói-se um novo triângulo  $DEF$ . O teorema de Napoleão afirma que, para qualquer triângulo  $ABC$ , o triângulo  $DEF$  é um triângulo *equilátero*.

Os dados essenciais que determinam um triângulo consistem em saber o comprimento de um lado e dois ângulos. Pelo uso da trigonometria podemos medir tudo o mais.

Na avaliação de superfícies de terras para traçar mapas é bastante útil pensar que “a Terra é chata” e supor que os triângulos sejam planos. Uma rede de triângulos é estabelecida, começando-se com uma linha de base  $BC$  de comprimento conhecido, escolhendo um ponto  $A$  distante (ponto de triangulação) e medindo os ângulos  $ABC$  e  $ACB$  por teodolito. Pela trigonometria sabe-se tudo a respeito do triângulo  $ABC$  e o topógrafo vai em frente, fixa o próximo ponto de triangulação a partir de uma nova linha de base  $AB$  ou  $AC$  e repete a operação para estabelecer uma teia de triângulos. O método tem a vantagem de ser capaz de mapear terrenos inóspitos que envolvam barreiras tais como pântanos, brejo, areia movediça e

rios.



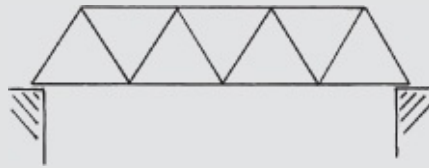
Teorema de Napoleão

O método foi usado como a base da Grande Inspeção Trigonométrica da Índia, que começou nos anos 1800 e durou 40 anos. O objetivo era avaliar e mapear ao longo do Grande Arco Meridional, do cabo Comorim, ao sul, e o Himalaia, ao norte, uma distância de umas 1.500 milhas. Para garantir a máxima exatidão na medida dos ângulos, sir George Everest providenciou a fabricação de dois teodolitos gigantes em Londres, pesando juntos uma tonelada e precisando de equipes com uma dúzia de homens para transportá-los. Era vital obter os ângulos certos. A precisão nas medidas era imprescindível e muito comentada, mas o centro das operações foi o humilde triângulo. Os vitorianos tiveram de passar sem GPS, embora tivessem computadores – ou homens que calculavam. Uma vez que todos os comprimentos em um triângulo tenham sido computados, o cálculo da área é direto. Mais uma vez, a unidade é o triângulo. Há diversas fórmulas para a área  $A$  de um triângulo, mas a mais notável é a fórmula de Heron de Alexandria:

## Construção com triângulos



O triângulo é indispensável na construção. Seu uso e força se baseia no fato que o tornou indispensável em levantamentos – um triângulo é rígido. Você consegue deformar um quadrado ou um retângulo, mas não um triângulo. Os andaimes usados em construções são uma união de triângulos, que também é vista como componente em tetos. Uma descoberta importante ocorreu na construção de pontes.



Uma ponte de viga de Warren

Uma ponte treliçada (viga de Warren) consegue aguentar grandes pesos, quando comparada a seu próprio peso. Ela foi patenteada em 1848 por James Warren, e a primeira ponte projetada desse modo foi construída na London Bridge Station dois anos mais tarde. O uso de triângulos equiláteros se provou mais confiável do que projetos semelhantes baseados em triângulos isósceles, em que apenas dois lados têm de ser iguais.

$$A = \sqrt{s \times (s - a) \times (s - b) \times (s - c)}$$

Ela pode ser aplicada a qualquer triângulo e não temos de conhecer nenhum ângulo. O símbolo  $s$  representa metade do perímetro do triângulo cujos lados são os comprimentos  $a$ ,  $b$  e  $c$ . Por exemplo, se um triângulo tem lados 13, 14 e 15, o perímetro é  $13 + 14 + 15 = 42$ , de modo que  $s = 21$ . Completando o cálculo,  $A = \sqrt{(21 \times 8 \times 7 \times 6)} = \sqrt{7.056} = 84$ . O triângulo é um objeto familiar, seja para crianças que brincam com formas simples ou para pesquisadores que lidam em bases diárias com a desigualdade de

triângulos na matemática abstrata. A trigonometria é a base para se fazer cálculos com triângulos, e as funções seno, cosseno e tangente são as ferramentas para descrevê-las, permitindo que façamos cálculos precisos para aplicações práticas. O triângulo recebeu muita atenção, mas é surpreendente que haja ainda tanta coisa esperando para ser descoberta a respeito de três linhas formando uma figura tão básica.

**A ideia condensada:  
três lados de uma  
história**

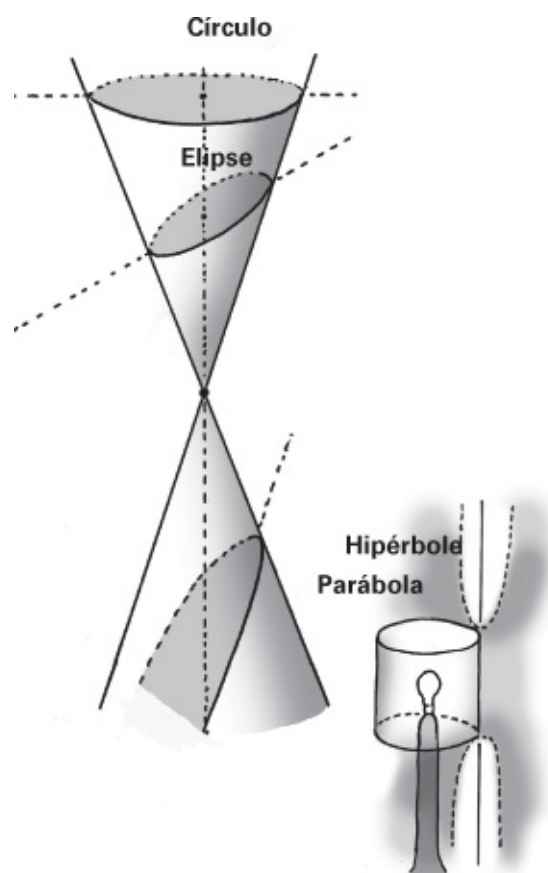
## 22 Curvas

### linha do tempo

c. 300 a.C.	c. 250 a.C.	c. 225 a.C.	1704 d.C.	1890	Década de 1920
Euclides define as secções cónicas	Arquimedes investiga as espirais	Apolônio de Parga publica <i>Cónicas</i>	Newton classifica as curvas cúbicas	Peano prova que um quadrado sólido é uma curva (curva de preenchimento especial)	Menger e Urysohn definem as curvas como parte da topologia.

**É fácil traçar uma curva. Artistas o fazem o tempo todo; arquitetos arrumam uma série de novos prédios na curva de um crescente ou de um cercado moderno. Um atirador de beisebol lança uma bola em curva. Os esportistas fazem arremesso em curva, e quando chutam para o gol, a bola segue uma curva. Mas, se perguntarmos “o que é uma curva?”, a resposta não é de tão fácil estruturação.**

Os matemáticos têm estudado curvas há séculos e a partir de diversos pontos de observação. Começou com os gregos, e as curvas que eles estudaram são agora chamadas de curvas “clássicas”.



Secções cónicas

**Curvas clássicas** A primeira família no reino das curvas clássicas são as chamadas “secções cónicas”. Os membros dessa família são o círculo, a elipse, a parábola e a hipérbole. A cônica é formada por um cone duplo, duas casquinhas de sorvete unidas, em que uma está de cabeça para baixo. Fatiando essa estrutura com um plano chato, as curvas da intersecção serão um círculo, uma elipse, uma parábola ou uma hipérbole, dependendo da inclinação do plano de corte ao eixo vertical do cone.

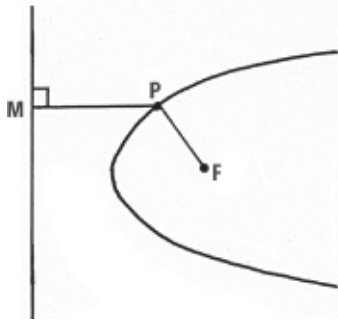
Podemos pensar em uma cônica como a projeção de um círculo em uma tela. Os raios de luz vindos do bulbo de uma lâmpada de mesa cilíndrica formam um cone de luz duplo, em que a luz vai jogar projeções das orlas circulares superiores e inferiores. A

imagem no teto será um círculo, mas se inclinarmos a lâmpada, esse círculo se transformará em uma elipse. Por outro lado, a imagem refletida contra a parede vai dar a curva em duas partes, a hipérbole.

As cônicas podem também ser descritas a partir do modo como pontos se movimentam no plano.

Esse é o método do “locus”, adorado pelos gregos, e ao contrário da definição da projeção, envolve comprimento. Se um ponto se movimenta de maneira que a distância entre ele e um ponto fixo é sempre a mesma, temos um círculo. Se um ponto se movimenta de modo que a soma de suas distâncias a dois pontos fixos (os focos) é um valor constante, temos uma elipse (quando os dois focos são iguais, a elipse se torna um círculo). A elipse foi a chave para o movimento dos planetas. Em 1609, o astrônomo alemão Johannes Kepler anunciou que os planetas giram em torno do sol em elipses, rejeitando a velha ideia de órbitas circulares.

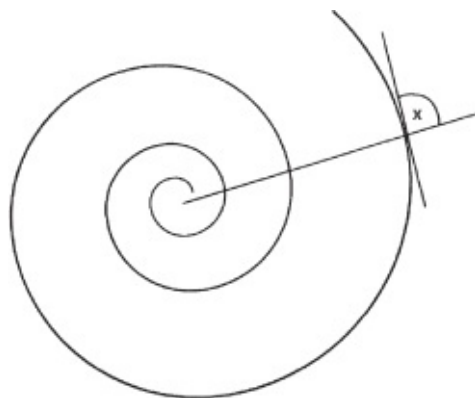
Menos óbvio é o ponto que se move de modo tal que a distância dele a um ponto (o foco  $F$ ) é a mesma que sua distância perpendicular a uma linha dada (a diretriz). Nesse caso temos uma parábola. A parábola tem uma multidão de propriedades úteis. Se uma fonte de luz é colocada no foco  $F$ , os raios da luz emitida são paralelos a  $PM$ . Por outro lado, se os sinais de TV são enviados por um satélite e atingem uma antena no formato de parábola, eles são reunidos no foco e mandados para o aparelho de TV.



A parábola

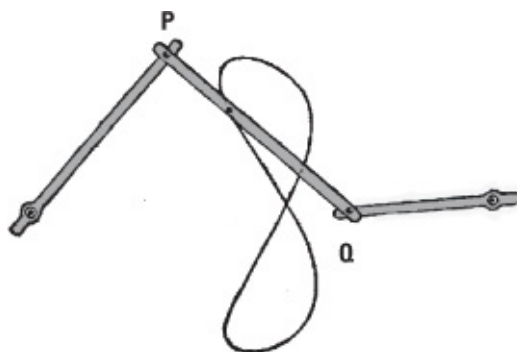
Se um bastão é rodado em torno de um ponto, qualquer ponto fixo no bastão traça um círculo, mas se um ponto é deixado para se mover para fora ao longo do bastão além de ele ser rodado ele vai gerar uma espiral. Pitágoras adorava a espiral, e mais tarde Leonardo da Vinci passou dez anos de sua vida estudando os diferentes tipos, enquanto René Descartes escreveu um tratado sobre elas. A espiral logarítmica é também chamada de espiral equiangular, porque faz o mesmo ângulo com o raio e a tangente no ponto em que o raio se encontra com a espiral.

Jacob Bernoulli, do famoso clã de matemáticos da Suíça, ficou tão extasiado com a espiral logarítmica que pediu que fosse gravada em seu túmulo, na Basileia. O “homem da Renascença” Emanuel Swedenborg considerava a espiral a mais perfeita das formas. Uma espiral tridimensional que gira em torno de um cilindro é chamada de hélice. Duas dessas – uma dupla hélice – forma a estrutura básica do DNA.



A espiral logarítmica

Há inúmeras curvas clássicas, como o limaçon, [“caracol de Pascal”], a lemniscata e os diversos ovais. A cardioide ganhou seu nome por ter o formato parecido ao de um coração. A curva catenária foi tema de pesquisa no século XVIII, identificada como a curva formada por uma cadeia pendurada entre dois pontos. A parábola é a curva vista em uma ponte suspensa pendurada entre dois pilões verticais.



Movimento de três barras

Um aspecto da pesquisa do século XIX sobre curvas foi a respeito daquelas curvas que eram geradas por bastões mecânicos. Esse tipo de questão era uma extensão do problema resolvido aproximadamente pelo engenheiro escocês James Watt, que projetou bastões unidos para transformar o movimento circular

em movimento linear. Na era do vapor, isso constituiu um progresso significativo.

O mais simples desses dispositivos mecânicos é o movimento de três bastões, em que os bastões são unidos com posições fixas a cada extremidade. Se a “barra acopladora”  $PQ$  se mover para qualquer lado, o loco de um ponto sobre ela acaba sendo uma curva de grau seis, uma “curva de sexta ordem”.

**Curvas algébricas** Seguindo Descartes, que revolucionou a geometria com a introdução de coordenadas  $x$ ,  $y$  e  $z$ , e os eixos cartesianos, batizados em sua homenagem, as cônicas poderiam agora ser estudadas como equações algébricas. Por exemplo, o círculo de raio 1 tem a equação  $x^2 + y^2 = 1$ , que é uma equação de segundo grau, como todas as cônicas. Um novo ramo da geometria cresceu, chamado de geometria algébrica.

Em um estudo importante, Isaac Newton classificou as curvas descritas por equações algébricas de grau três de curvas cúbicas. Comparadas com as quatro cônicas básicas, foram encontrados 78 tipos, agrupados em cinco classes. A explosão do número de tipos diferentes continua para as curvas de quarto grau, com tantos tipos diferentes que uma classificação completa nunca foi efetuada.

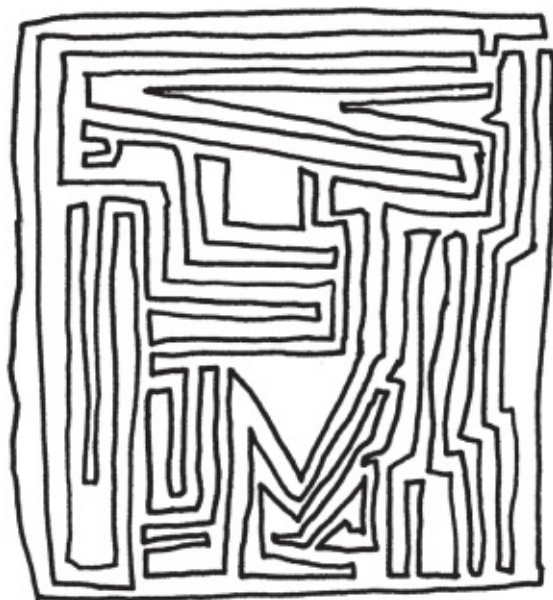
O estudo das curvas como equações algébricas não é a história toda. Muitas curvas, como a catenária, as cicloides (curvas traçadas por um ponto em uma roda girando) e espirais não são fáceis de se exprimir como equações algébricas.

**Uma definição** O que os matemáticos estavam buscando era uma definição de curva, não apenas exemplos específicos. Camille



Jordan propôs uma teoria de curvas construída na definição de uma curva em termos de pontos variáveis.

Eis um exemplo. Se fazemos  $x = t^2$  e  $y = 2t$ , então, para diferentes valores de  $t$  obtemos muitos pontos diferentes, que podemos escrever como coordenadas  $(x, y)$ . Por exemplo, se  $t = 0$ , temos o ponto  $(0, 0)$ ,  $t = 1$  dá o ponto  $(1, 2)$ , e daí por diante. Se lançarmos em gráfico esses pontos nos eixos  $x$ - $y$  e “unirmos os pontos” vamos obter uma parábola. Jordan refinou essa ideia de se traçar pontos. Para ele isso era a definição de uma curva.



Uma curva de Jordan simples fechada

As curvas de Jordan podem ser intrincadas, mesmo quando são como o círculo, no sentido de que são “simples” (não se cruzam) e “fechadas” (não têm começo nem fim). O famoso teorema de Jordan tem sentido. Ele afirma que uma curva simples fechada tem um lado de fora e um lado de dentro. Sua aparente “obviedade” é uma ilusão.

Na Itália, Giuseppe Peano causou sensação quando, em 1890, mostrou que, de acordo com a definição de Jordan, um quadrado preenchido é uma curva. Ele conseguia arrumar os pontos em um quadrado de modo que *todos* poderiam ser “cortados” e ao mesmo tempo obedecer à definição de Jordan. Isso foi chamado de curva de preenchimento espacial e detonou a definição de Jordan – claramente um quadrado não é uma curva no sentido convencional.

Exemplos de curvas de preenchimento espacial e outros exemplos patológicos fizeram com que matemáticos voltassem à prancheta de desenho mais uma vez e pensassem a respeito dos fundamentos da teoria da curva. Foi levantada a questão toda de desenvolver uma definição melhor para curva. No início do século XX, essa tarefa levou a matemática para o novo campo da topologia.

## A ideia condensada:

**saindo pela tangente**

## 23 Topologia

### linha do tempo

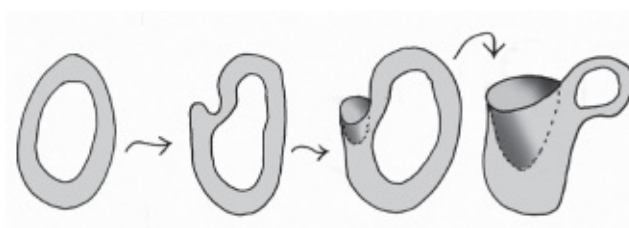
c. 300 a.C.	c. 250 a.C.	1752 d.C.	1858	1961	1982	2002
Euclides demonstra que há cinco poliedros regulares	Arquimedes investiga os poliedros truncados	Euler dá sua fórmula para o número de vértices, arestas e faces em um poliedro	Möbius e Listing introduzem a fita de Möbius	Stephen Smale prova a conjectura de Poincaré em dimensões maiores do que 4	Michael Freedman prova a conjectura de Poincaré em dimensões iguais a 4	Grigori Perelman prova a conjectura de Poincaré para a dimensão 3

**A topologia é o ramo da geometria que lida com as propriedades de superfícies e formas em geral, mas não engloba medidas de comprimentos ou ângulos.**

**Destacam-se as qualidades que não mudam quando formatos são transformados em outros formatos.**

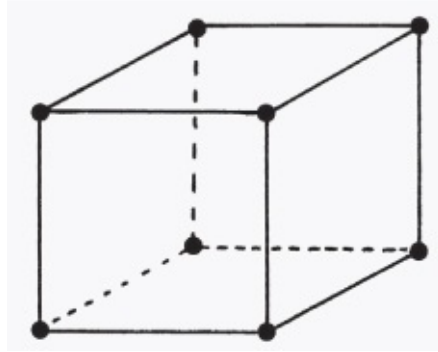
**Podemos empurrar e puxar o formato em qualquer direção e por isso a topologia é algumas vezes descrita como a “geometria da folha de borracha”. Topólogos são pessoas que não conseguem perceber a diferença entre uma rosca e uma xícara de café!**

Uma rosca é uma superfície dotada de um só buraco. Uma xícara de café é a mesma coisa, mas o buraco toma a forma de uma alça. Eis aqui como uma rosca pode ser transformada em uma xícara de café.



**Classificação de poliedros** Os formatos mais básicos estudados pelos topógrafos são os poliedros (*poli* significa “muitos” e *hedra* significa “faces”). Um exemplo de poliedro é um cubo, com 6 faces quadradas, 8 vértices (pontos na junção das faces) e 12

arestas (as linhas que unem os vértices). O cubo é um poliedro *regular* porque: Todas as faces têm o mesmo formato regular Todos os ângulos entre as arestas que se encontram em um



vértice são iguais

A topologia é um assunto relativamente novo, mas ainda assim remonta aos gregos e, na verdade, o resultado culminante dos *Elementos* de Euclides é mostrar que há exatamente cinco poliedros regulares. Eles são os sólidos platônicos: Tetraedro (com 4 faces triangulares) Cubo (com 6 faces quadradas) Octaedro (com 8 faces triangulares) Dodecaedro (com 12 faces pentagonais) Icosaedro (com 20 faces triangulares)



Tetraedro



Cubo



Octaedro





Dodecaedro



Icosaedro

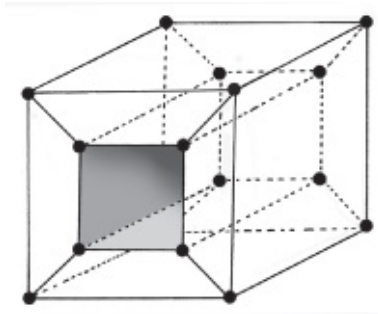


## Icosaedro truncado

Se eliminarmos a condição de que todas as faces sejam iguais, estamos no reino dos sólidos de Arquimedes, que são semirregulares. Exemplos deles podem ser gerados a partir dos sólidos platônicos. Se cortarmos (truncarmos) alguns cantos do icosaedro, temos o formato usado como projeto da moderna bola de futebol. As 32 faces que formam os painéis são feitas de 12 pentágonos e 20 hexágonos. Há 90 arestas e 60 vértices. É também o formato das moléculas de buckminsterfulereno, batizada em homenagem ao visionário Richard Buckminster Fuller, criador do domo geodésico. Essas “*bucky-balls*” são uma forma recém-descoberta de carbono, o  $C_{60}$ , com um átomo de carbono encontrado em cada vértice.

**Fórmula de Euler** A fórmula de Euler é o número de vértices  $V$ , arestas  $E$  e faces  $F$  de um poliedro, conectados pela fórmula  $V - E + F = 2$

Por exemplo, para um cubo,  $V = 8$ ,  $E = 12$ , e  $F = 6$ , de modo que  $V - E + F = 8 - 12 + 6 = 2$  e, para as moléculas de buckminsterfulereno,  $V - E + F = 60 - 90 + 32 = 2$ . Esse teorema, na verdade, desafia a própria noção de poliedro.



O cubo com um túnel

Se um cubo for atravessado por um “túnel”, ele é um poliedro verdadeiro? Para esse formato,  $V = 16$ ,  $E = 32$ ,  $F = 16$  e  $V - E + F = 16 - 32 + 16 = 0$ , a fórmula de Euler não funciona. Para reivindicar a exatidão da fórmula, o tipo de poliedro pode ser limitado àqueles sem túneis; ou, como alternativa, a fórmula poderia ser generalizada para incluir essa peculiaridade.

**Classificação de superfícies** Um topógrafo poderia encarar a rosca e a xícara de café como idênticas, mas que tipo de superfície é diferente da rosca? Uma candidata seria uma bola de borracha. Não há como transformar a rosca em uma bola, já que a rosca tem um buraco e a bola, não. Isso é uma diferença fundamental entre duas superfícies. Então, o jeito de classificar superfícies é pelo número de buracos que elas contêm.

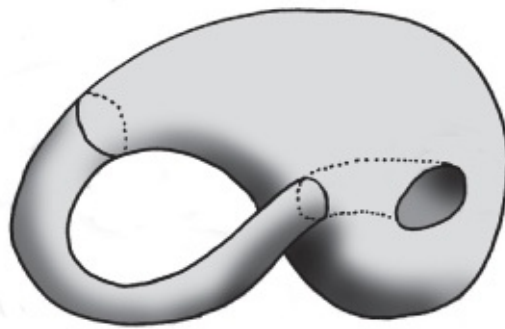
Vamos tomar uma superfície com  $r$  buracos e dividi-la em regiões ligadas por arestas unindo vértices, plantados na superfície. Uma vez feito isso, podemos contar o número de vértices, arestas e faces. Para qualquer divisão, a expressão de Euler  $V - E + F$  tem sempre o mesmo valor, chamado de característica Euler da superfície:  $V - E + F = 2 - 2r$

Se a superfície não tiver buraco algum ( $r = 0$ ) como era o caso de poliedros comuns, a fórmula se reduz a  $V - E + F = 2$  de Euler. No caso de um buraco ( $r = 1$ ), como no caso do cubo com um túnel,  $V - E + F = 0$ .



Fita de Möbius

**Superfícies com só um lado** Em geral, uma superfície tem dois lados. O lado de fora de uma bola é diferente do lado de dentro e o único jeito de passar de um lado para o outro é fazer um furo na bola – uma operação de corte que não é permitida na topologia (você pode esticar, mas não pode cortar). Uma folha de papel é outro exemplo de uma superfície com dois lados. O único local onde um lado se encontra com o outro é ao longo da curva delimitadora formada pelas beiradas do papel.



## Garrafa de Klein

A ideia de uma superfície de só um lado parece improvável. Mesmo assim, foi descoberta uma famosa, pelo matemático e astrônomo alemão August Möbius no século XIX. O modo de construir tal superfície é tomar uma tira de papel, dar uma torcida e unir as extremidades. O resultado é uma “fita de Möbius”, uma superfície de só um lado com uma curva delimitadora. Você pode pegar um lápis e começar a desenhar uma linha ao longo do meio dela. Logo você vai estar de volta ao ponto em que começou!

É possível até ter uma superfície de um só lado, sem uma curva delimitadora. É a “garrafa de Klein”, cujo nome foi dado em homenagem ao matemático alemão Felix Klein. O que é especialmente impressionante a respeito dessa garrafa é que ela não se intersecta. Entretanto, não é possível fazer seu modelo no espaço tridimensional sem uma intersecção física, porque ela está devidamente em quatro dimensões, e não haveria intersecções.

Essas duas superfícies são exemplos do que os topógrafos chamam de “*variedades*” (“*manifolds*”, em inglês) – superfícies geométricas que parecem pedaços de papel bidimensionais quando porções pequenas são vistas sozinhas. Já que a garrafa de Klein não tem limites, é chamada de 2-*manifolds* “fechados”.

**A conjectura de Poincaré** Durante mais de um século, um problema proeminente na topologia foi a famosa conjectura de Poincaré, batizada em homenagem a Henri Poincaré. A conjectura está centrada na conexão entre álgebra e topologia.

A parte da conjectura que permaneceu sem solução até recentemente se aplicava a *3-manifolds* fechados. Eles podem ser complicados – imagine uma garrafa de Klein com uma dimensão a mais. Poincaré conjecturou que determinados *3-manifolds* fechados que apresentassem todas as marcas algébricas de serem esferas tridimensionais tinham na realidade de ser esferas. Era como se você andasse em torno de uma bola gigante e todas as pistas lhe indicassem ser uma esfera, mas como não conseguia ver a imagem total, você ficava pensando se era mesmo uma esfera.

Ninguém conseguiu provar a conjectura de Poincaré para *3-manifolds*. Era verdadeira ou era falsa? Já foi provado para todas as demais dimensões, mas o caso dos *3-manifolds* é instigante. Houve muitas provas falsas até 2002, quando se reconheceu que Grigori Perelman, do Instituto Steklov em São Petersburgo, tinha finalmente encontrado a prova. Do mesmo modo que a solução de outros grandes problemas em matemática, as técnicas de solução para a conjectura de Poincaré ficam fora de sua área imediata, em uma técnica chamada de difusão de calor.

**A ideia condensada:  
de roscas a xícaras  
de café**

## 24 Dimensão

### linha do tempo

c.300 a.C.	1877 d.C.	1909	1919	1970
Euclides descreve um mundo tridimensional	Cantor se surpreende com suas controversas descobertas na teoria da dimensão	O trabalho de Brouwer muda a nossa noção de dimensão	Hausdorff introduz a noção de "dimensão Hausdorff" fracional	A teoria das cordas concebe nosso universo como tendo 10, 11 e 26 dimensões

**Leonardo da Vinci escreveu em seu caderno: “A ciência de pintar começa no ponto, depois vem a linha, o plano vem em terceiro lugar e o quarto é o corpo em sua vestimenta de planos”. Na hierarquia de Da Vinci, o ponto tem dimensão zero, a linha é unidimensional, o plano é bidimensional e o espaço é tridimensional. O que pode ser mais óbvio? Foi o modo pelo qual a geometria do ponto, da linha, do plano e do sólido foi propagada pelo geômetra grego Euclides, e Leonardo estava seguindo a apresentação de Euclides.**

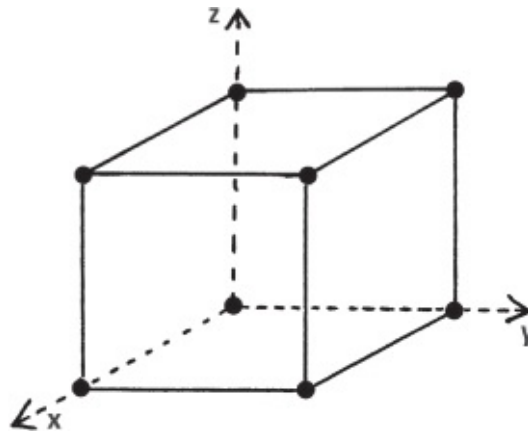
Há milênios a percepção é que o espaço físico é tridimensional. No espaço físico é possível *sair* desta página ao longo do eixo dos  $x$  ou através dele horizontalmente ao longo do eixo dos  $y$ , ou verticalmente subindo pelo eixo de  $z$ , ou qualquer combinação desses. Com relação à origem (onde os três eixos se encontram), cada ponto tem um conjunto de coordenadas espaciais especificadas por valores de  $x$ ,  $y$  e  $z$ , escritas sob a forma

$$(x, y, z)$$

Um cubo claramente tem essas três dimensões, bem como tudo mais que seja sólido. Em geral, na escola nos ensinam a geometria do plano, que é bidimensional, e depois passamos para as três dimensões – para “geometria dos sólidos” e



paramos por aí.



O espaço de três dimensões

Por volta do começo do século XIX, os matemáticos começaram a explorar em quatro dimensões e em matemáticas de dimensões  $n$  mais altas. Muitos filósofos e matemáticos começaram a perguntar se existiriam dimensões mais altas.

**Dimensões físicas mais altas** Muitos dos principais matemáticos no passado achavam que quatro dimensões não poderiam ser imaginadas. Eles punham em dúvida a realidade de quatro dimensões, cuja explicação se tornou um desafio.

Um modo comum de explicar porque quatro dimensões podiam ser possíveis era cair de volta nas duas dimensões. Em 1884, um professor de colégio e teólogo inglês, Edwin Abbott, publicou um livro muito popular a respeito de “*terraplanários*”, que viviam no plano bidimensional (terra plana). Eles não conseguiam ver os triângulos, quadrados ou círculos que existiam na *Terraplana* (*Flatland*, no original) porque não podiam ir vê-los do ponto de vista da terceira dimensão. A visão deles era severamente limitada. Eles tinham os mesmos problemas em pensar sobre a

terceira dimensão que nós temos em pensar em uma quarta. Mas a leitura de Abbott nos põe em um estado mental para aceitar a quarta dimensão.

A necessidade de contemplar a existência real de um espaço de quatro dimensões se tornou mais urgente quando Einstein entrou em cena. A geometria tetradimensional se tornou mais plausível, e até mais compreensível, porque a dimensão extra no modelo de Einstein é o *tempo*. Diferentemente de Newton, Einstein concebeu o tempo como unido com o espaço em um *continuum* tetradimensional espaço-tempo. Einstein decretou que vivemos em um mundo tetradimensional com quatro coordenadas  $(x, y, z, t)$ , onde  $t$  designa o tempo.

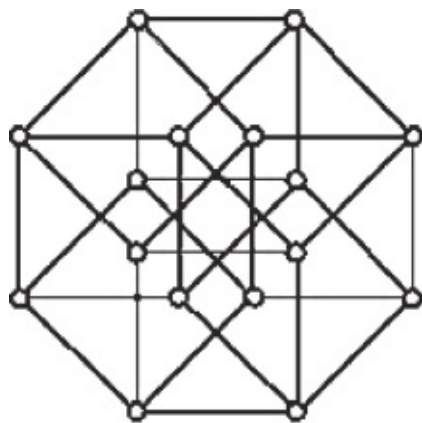
Hoje em dia o mundo tetradimensional de Einstein parece bastante tranquilo e corriqueiro. Um modelo mais recente de realidade física é baseado em “cordas”. Nessa teoria, as familiares partículas subatômicas, como os elétrons, são manifestações de cordas em vibrações extremamente pequenas. A teoria das cordas sugere uma substituição do *continuum* espaço-tempo tetradimensional por uma versão de dimensão mais alta. Pesquisas atuais sugerem que a dimensão do complacente *continuum* espaço-tempo para a teoria das cordas deveria ser 10, 11 ou 26, dependendo de mais suposições e pontos de vista diferentes.

Um imenso magneto de 2 mil toneladas no CERN, perto de Genebra, na Suíça, projetado para provocar colisões de partículas em altas velocidades, poderia ajudar a resolver a questão. O propósito é descobrir a estrutura da matéria e, como subproduto,

apontar para uma teoria melhor e para a resposta “correta” para a dimensionalidade. A especulação é que estamos vivendo em um universo de dimensão 11.

**Hiperespaço** Diferentemente de dimensões físicas mais altas, não há absolutamente qualquer problema com um *espaço matemático* de mais do que três dimensões. O espaço matemático pode ter qualquer número de dimensões. Desde o início do século XIX matemáticos têm habitualmente usado  $n$  variáveis em seu trabalho. George Green, um moleiro de Nottingham que explorou a matemática da eletricidade, e os matemáticos puros A.I. Cauchy, Arthur Cayley e Hermann Grassmann, descreveram, todos, sua matemática em termos de hiperespaços  $n$ -dimensionais. Parece não haver nenhuma boa razão para limitar a matemática, e tudo a ser ganho em elegância e clareza.

A ideia por trás de  $n$  dimensões é meramente uma extensão das coordenadas tridimensionais  $(x, y, z)$  para um número não especificado de variáveis. Um círculo em duas dimensões tem uma equação  $x^2 + y^2 = 1$ , uma esfera em três dimensões tem uma equação  $x^2 + y^2 + z^2 = 1$ , então por que não uma hiperesfera em quatro dimensões com equação  $x^2 + y^2 + z^2 + w^2 = 1$ ?



## O cubo tetradimensional

Os oito vértices de um cubo em três dimensões têm coordenadas da forma  $(x, y, z)$  onde cada um dos  $x, y, z$  são ou 0 ou 1. O cubo tem seis faces, cada uma das quais é um quadrado, e há  $2 \times 2 \times 2 = 8$  vértices. E um cubo tetradimensional? Ele terá coordenadas da forma  $(x, y, z, w)$  onde cada um dos  $x, y, z, w$  são ou 0 ou 1. Então há  $2 \times 2 \times 2 \times 2 = 16$  arestas possíveis para o cubo tetradimensional, e oito faces, e cada uma é um cubo. Não podemos na realidade ver esse cubo tetradimensional, mas é possível criar a impressão de um artista sobre ele em uma folha de papel. Isso mostra uma projeção do cubo tetradimensional que existe na imaginação do matemático. As faces cúbicas mal podem ser percebidas.

Um espaço matemático de muitas dimensões é uma ocorrência bastante comum para os matemáticos puros. Ninguém alega sua existência real, embora em um mundo platônico possa se supor que exista. No grande problema da classificação de grupos, por exemplo (ver p. 157), o “grupo monstro” é um modo de medir simetria no espaço matemático de 196.883 dimensões. Não conseguimos “ver” esse espaço da mesma maneira que vemos no espaço tridimensional comum, mas mesmo assim ele pode ser imaginado e pode-se lidar com ele de modo preciso através da álgebra moderna.

O interesse matemático pela dimensão é inteiramente separado do significado que o físico liga à análise dimensional. As unidades comuns da física são medidas em termos de massa  $M$ , comprimento  $L$  e tempo  $T$ . Então, usando a análise dimensional

dele, um físico pode verificar se equações fazem sentido, já que os dois lados de uma equação têm de ter as mesmas dimensões.

Não é uma boa ter força = velocidade. Uma análise dimensional dá a velocidade como metros por segundo, de modo que tem dimensões de comprimento divididas pelo tempo, ou  $L/T$ , que escrevemos como  $LT^{-1}$ . Força é massa vezes aceleração, e como aceleração é metros por segundo por segundo, o resultado líquido é que força terá dimensões  $MLT^{-2}$ .

## Pessoas coordenadas

Os próprios seres humanos são multidimensionais. Um ser humano tem muito mais “coordenadas” do que três. Podemos usar  $(a, b, c, d, e, f, g, h)$  para idade, altura, peso, gênero, tamanho do sapato, cor dos olhos, cor dos cabelos, nacionalidade e daí por diante. Em lugar de pontos geométricos podemos ter gente. Se nos limitarmos a esse “espaço” de oito dimensões de pessoas, John Doe poderia ter coordenadas como (43 anos, 165 cm, 83 kg, masculino, 41, azuis, louro, dinamarquês) e as coordenadas da Mary Smith poderiam ser (26 anos, 157 cm, 56 kg, feminino, 33, castanho, morena, britânica).

**Topologia** A teoria da dimensão faz parte da topologia geral. Outros conceitos de dimensão podem ser definidos de modo independente, em termos de espaços matemáticos abstratos. Uma tarefa importante é mostrar como eles se relacionam uns com os outros. Figuras proeminentes em diversos ramos da matemática investigaram o significado das dimensões, inclusive Henri Lebesgue, L.E.J Brouwer, Karl Menger, Pavel Urysohn e Leopold Vietoris (que chegou a ser a pessoa mais velha na Áustria e morreu em 2002 com 110 anos de idade).

O livro central sobre o assunto foi *Dimension Theory* (Teoria da dimensão). Publicado em 1948 por Witold Hurewicz e Henry Wallman, ainda é visto como um divisor de águas na nossa compreensão do conceito de dimensão.

**Dimensão sob todas as suas formas** A partir das três dimensões

introduzidas pelos gregos, o conceito de dimensão tem sido criticamente analisado e ampliado.

As  $n$  dimensões do espaço matemático foram introduzidas de modo bastante indolor, enquanto os físicos basearam suas teorias no espaço-tempo (quarta dimensão) e versões recentes da teoria das cordas (ver p. 99) que exige 10, 11 e 26 dimensões. Incursões têm sido feitas em dimensões fracionárias com formatos fractais (ver p. 102) estudando-se diversas medidas diferentes. Hilbert introduziu um espaço matemático de dimensão infinita que agora é a estrutura básica para os matemáticos puros. A dimensão é tão mais do que o um-dois-três da geometria euclidiana.

## **A ideia condensada: além da terceira dimensão**

## 25 Fractais

### linha do tempo

1879 d.C.	1904	1918	1919	1975
Cayley trabalha em um precursor dos fractais modernos	von Koch cria sua curva do floco de neve	Hausdorff introduz seu conceito de dimensão fracionária	Julia e Fatou investigam estruturas fractais no plano complexo	Mandelbrot introduz o termo fractal

**Em março de 1980, o computador principal mais moderno no centro de pesquisa da IBM em Yorktown Heights, no estado de Nova York, estava enviando suas instruções para um antigo dispositivo de impressão Tektronix. O dispositivo obediamente traçava pontos em locais curiosos em uma página em branco, e quando silenciou, o resultado parecia ser um punhado de areia borrado sobre a folha. Benoît Mandelbrot esfregou os olhos sem querer acreditar. Ele percebeu que era importante, mas o que era aquilo? A imagem que lentamente aparecia à sua frente era como o impresso em preto e branco emergindo de um banho de revelação fotográfica. Era o primeiro vislumbre do ícone no mundo dos fractais – o conjunto de Mandelbrot.**

Isso era matemática experimental por excelência, uma abordagem ao assunto em que os matemáticos tinham suas bancadas de laboratório exatamente como os físicos e químicos. Eles agora também podiam fazer experiências. Abriram-se novas vistas – literalmente. Era uma liberação dos áridos climas de “definição, teorema, prova”, embora fosse necessária uma volta aos rigores do argumento racional, mesmo que mais adiante.



O avesso dessa abordagem experimental era que as imagens visuais precediam um embasamento teórico. Os experimentalistas estavam navegando sem mapa. Embora Mandelbrot tivesse cunhado a palavra “fractais”, o que eram eles? Será que podiam ser definidos com precisão, no modo usual da matemática? No começo, Mandelbrot não queria fazer isso. Ele não queria destruir a mágica da experiência afiando uma definição aguçada que pudesse ser inadequada e limitante. Ele sentiu que a noção de fractal era “como um bom vinho – exigia um pouco de envelhecimento antes de ser ‘engarrafada’”.

**O conjunto de Mandelbrot** Mandelbrot e seus colegas não estavam sendo matemáticos de compreensão particularmente difícil. Eles estavam brincando com a mais simples das fórmulas. A ideia toda era baseada na iteração – a prática de aplicar uma fórmula repetidas vezes. A fórmula que gerou o conjunto de Mandelbrot era simplesmente  $x^2 + c$ .

A primeira coisa que fazemos é escolher um valor para  $c$ . Vamos escolher  $c = 0,5$ . Começando com  $x = 0$ , fazemos a substituição na fórmula  $x^2 + 0,5$ . Esse primeiro cálculo dá outra vez  $0,5$ . Agora usamos isso como  $x$ , substituindo em  $x^2 + 0,5$  para obter um segundo cálculo:  $(0,5)^2 + 0,5 = 0,75$ . Continuamos com isso, e no terceiro estágio teremos  $(0,75)^2 + 0,5 = 1,0625$ . Todos esses cálculos podem ser feitos em uma calculadora de mão. Continuando, vemos que a resposta fica cada vez maior.

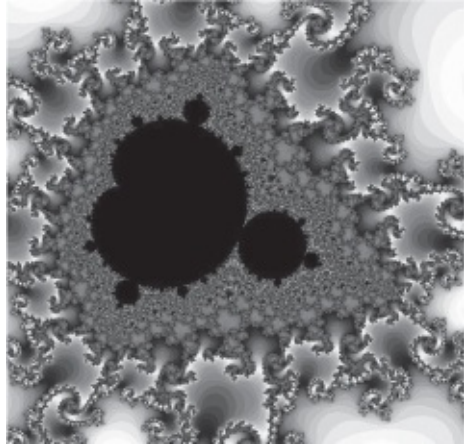
Vamos tentar outro valor para  $c$ , dessa vez  $c = -0,5$ . Como antes, começamos com  $x = 0$  e substituímos em  $x^2 - 0,5$  para dar  $-0,5$ . Continuando, obtemos  $-0,25$ , mas dessa vez os valores não

ficam cada vez maiores, mas, depois de algumas oscilações, estabilizam-se em torno de um número próximo de  $-0,3660$ ...

Então, escolhendo  $c = 0,5$ , a sequência que começa em  $x = 0$  dispara para o infinito, mas escolhendo  $c = -0,5$  encontramos que a sequência começando por  $x = 0$  na verdade converge para um valor próximo a  $-0,3660$ . O conjunto de Mandelbrot consiste em todos os valores de  $c$  para os quais a sequência começando em  $x = 0$  não foge para o infinito.

Essa não é a história toda, porque até agora só consideramos números reais de uma dimensão – dando um conjunto de Mandelbrot unidimensional, de modo que não vemos muita coisa. O que tem de ser considerado é a mesma fórmula  $z^2 + c$ , mas  $z$  e  $c$  sendo números complexos bidimensionais (ver p. 34). Isso nos dará um conjunto de Mandelbrot bidimensional.

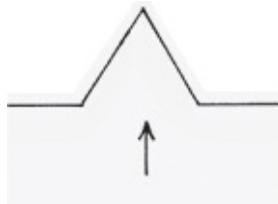
Para alguns valores de  $c$  no conjunto de Mandelbrot, a sequência de  $z$ s pode fazer todo tipo de coisas estranhas, como dançar entre um número de pontos, mas eles não fugirão para o infinito. No conjunto de Mandelbrot, vemos ainda outra propriedade-chave dos fractais, a da autossimilaridade. Se você der um *zoom* no conjunto, não saberá ao certo qual o nível de ampliação porque você vai ver apenas mais conjuntos de Mandelbrot.



## O conjunto de Mandelbrot

**Antes de Mandelbrot** Como a maior parte das coisas em matemática, as descobertas raramente são inteiramente novas. Examinando a história, Mandelbrot descobriu que matemáticos como Henri Poincaré e Arthur Cayley tiveram breves lampejos da ideia dos fractais cem anos antes dele. Infelizmente eles não tinham o poder computacional para investigar as questões mais a fundo.

Os formatos descobertos pela primeira onda dos teóricos dos fractais incluíam curvas enrugadas e “curvas monstro”, que tinham anteriormente sido desconsideradas como exemplos patológicos de curvas. Como elas eram assim tão patológicas, foram trancadas no armário dos matemáticos sem receber muita atenção. O que se queria então eram curvas mais suaves, “macias”, normais, que pudessem ser lidadas por cálculo diferencial. Com a popularidade dos fractais, outros matemáticos cujos trabalhos foram ressuscitados foram Gaston Julia e Pierre Fatou, que trabalharam com estruturas parecidas com os fractais em planos complexos nos anos que se seguiram à Primeira Guerra Mundial. As curvas deles não eram chamadas de fractais, é claro, e eles não tinham o equipamento tecnológico para ver o formato delas.

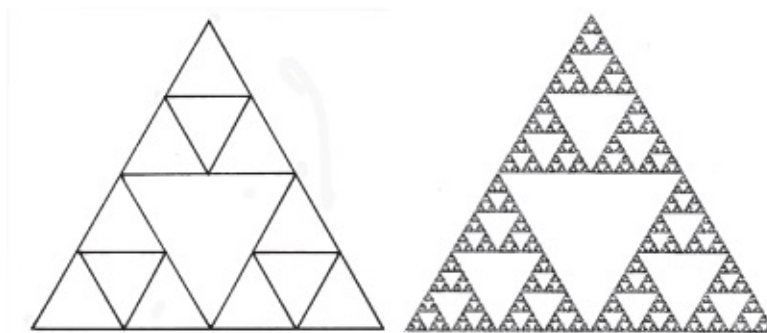


O elemento gerador do floco de neve de Koch

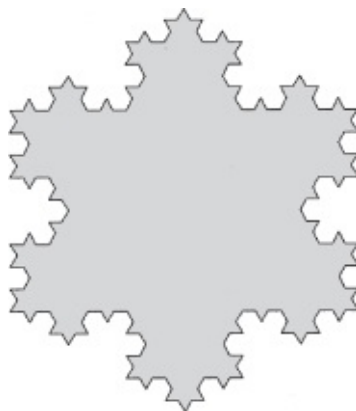
**Outros fractais famosos** A famosa curva de Koch teve o nome do matemático sueco Niels Fabian Helge von Koch. A curva do floco de neve, praticamente a primeira curva fractal, é gerada a partir do lado do triângulo tratado como um elemento, dividindo-o em três partes, cada um de comprimento  $1/3$  e acrescentando um triângulo na posição do meio.

A propriedade curiosa da curva de Koch é que ela tem uma área finita, porque sempre fica dentro de um círculo, mas em cada estágio de sua geração o comprimento aumenta. É uma curva que encerra uma área finita, mas tem uma circunferência “infinita”!

Outro fractal famoso recebeu o nome do matemático polonês Wacław Sierpinski. Ele é obtido subtraindo-se triângulos de um triângulo equilátero; e continuando esse processo, obtemos a gaxeta de Sierpinski (gerada por um processo diferente na p. 56).



A gaxeta de Sierpiński



O floco de neve de Koch

**Dimensão fracionária** O modo pelo qual Felix Hausdorff examinou a dimensão foi inovador. Tinha a ver com escala. Se uma linha é ampliada por um fator de 3, ela é 3 vezes mais comprida do que era antes. Como  $3 = 3^1$  uma linha é dita ter dimensão 1. Se um quadrado sólido é ampliado por um fator de 3, sua área é 9 vezes seu valor anterior de  $3^2$ , então a dimensão é 2. Se um cubo é ampliado por esse valor, seu volume é 27 ou  $3^3$  vezes seu valor anterior, de modo que sua dimensão é 3. Esses valores da dimensão de Hausdorff coincidem todos com nossas expectativas para uma linha, um quadrado ou um cubo.

Se a unidade básica da curva de Koch for ampliada em uma escala 3, ela se torna 4 vezes mais longa do que era antes. Seguindo o esquema descrito, a dimensão de Hausdorff é o valor de  $D$  para o qual  $4 = 3^D$ . Um cálculo alternativo é que

$$D = \frac{\log 4}{\log 3}$$

Isso significa que para a curva de Koch  $D$  é aproximadamente 1,262. Com os fractais frequentemente ocorre que a dimensão de Hausdorff é maior do que a dimensão comum, que é 1 no caso da

curva de Koch.

A dimensão de Hausdorff propagou a definição de Mandelbrot de um fractal – um conjunto de pontos cujo valor de  $D$  não é um número inteiro. Dimensões fracionárias se tornaram a principal propriedade dos fractais.

**As aplicações dos fractais** O potencial para as aplicações dos fractais é amplo. Fractais podem muito bem ser o meio matemático para modelos do tipo objetos naturais, como o crescimento de plantas ou a formação de nuvens.

Fractais já foram aplicados ao crescimento de organismos marinhos, como corais e esponjas. O espalhamento de cidades modernas tem sido mostrado como tendo uma semelhança com o crescimento fractal. Na medicina já encontraram aplicação na modelagem da atividade cerebral. E a natureza fractal do movimento de ações e o mercado de câmbio exterior também tem sido investigado. O trabalho de Mandelbrot abriu toda uma nova visão e ainda há muito a ser descoberto.

**A ideia condensada:  
formatos com  
dimensão fracionária**

## 26 Caos

### linha do tempo

1812 d.C.	1889	1961	1971	2004
Laplace publica seu ensaio sobre um mundo determinístico	Poincaré encontra caos em seu trabalho sobre o problema de três corpos pelo qual ele ganha um prêmio do rei Oscar da Suécia	Lorenz observa o efeito borboleta	Robert May investiga caos em modelos populacionais	A teoria do caos alcança a cultura popular no filme <i>O efeito borboleta</i>

**Como é possível haver uma teoria do caos? O caos não ocorre justamente na ausência de teoria? A história remonta a 1812. Enquanto Napoleão avançava sobre Moscou, seu compatriota, o marquês Pierre-Simon de Laplace, publicou um ensaio a respeito do universo determinístico: se, em um determinado instante, as posições e velocidades de todos os objetos no universo fossem conhecidas, e também as forças que agem sobre eles, então essas quantidades poderiam ser calculadas com exatidão para todos os momentos futuros. O universo e todos os objetos dentro dele seriam completamente determinados. A teoria do caos nos mostra que o mundo é mais intrincado do que isso.**

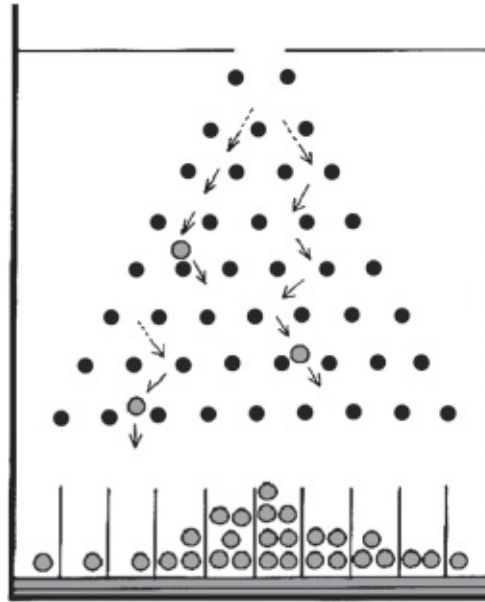
No mundo real não podemos conhecer todas as posições, velocidades e forças com exatidão, mas o corolário à crença de Laplace era que se soubermos valores aproximados em um instante, o universo não seria muito diferente, de qualquer modo. Isso era razoável porque, com toda a certeza, corredores de velocidade que comesçassem um décimo de segundo depois de dada a partida só quebrariam a fita um décimo de segundo depois de seu tempo habitual. A crença era que pequenas discrepâncias em condições iniciais significariam pequenas discrepâncias nos resultados. A teoria do caos detonou essa



ideia.

**O efeito borboleta** O efeito borboleta mostra como condições iniciais ligeiramente diferentes das condições dadas podem produzir um resultado real muito diferente do predito. Se é previsto tempo bom para um dia na Europa, mas uma borboleta bate as asas na América do Sul, então isso pode pressagiar tempestades do outro lado do mundo – porque o bater das asas muda a pressão do ar muito ligeiramente, provocando um padrão meteorológico bem diferente da previsão original.

É possível ilustrar essa ideia com uma simples experiência mecânica. Se você deixar cair uma pedrinha através da abertura no topo de uma caixa de pinos, ela vai avançar para baixo, sendo desviada para um lado ou para o outro pelos diferentes pinos que encontrar pelo caminho até entrar em uma fenda ao fundo. Você pode tentar deixar uma outra pedra idêntica cair da mesma posição com exatamente a mesma velocidade. Se você conseguir fazer isso *exatamente*, então o marquês de Laplace estaria correto e o trajeto seguido pela bola seria exatamente o mesmo. Se a primeira bola caísse na terceira fenda à esquerda, então a segunda também cairia lá.



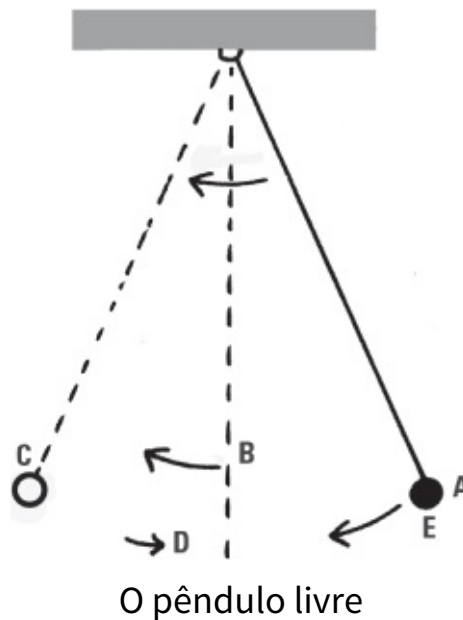
Experiência da *pinboard*

Mas é claro que você não consegue fazer a bola cair exatamente da mesma posição com exatamente a mesma velocidade e força. Na realidade, haverá uma ligeira diferença que você não poderá sequer ser capaz de medir. O resultado é que a pedra poderá seguir uma rota muito diferente até o fundo e provavelmente terminar em uma fenda diferente.

**Um pêndulo simples** Um pêndulo simples é um dos sistemas mecânicos mais simples para se analisar. À medida que o pêndulo oscila para trás e para a frente, ele aos poucos perde energia. O deslocamento da vertical e a velocidade (angular) do pêndulo diminuem até que ele eventualmente fique estacionário.

O movimento do peso do pêndulo pode ser traçado em um diagrama de fase. No eixo horizontal mede-se o deslocamento (angular) e no eixo vertical se mede a velocidade. O ponto de lançamento é marcado no ponto A do eixo horizontal positivo. Em A o deslocamento está no máximo e a velocidade é zero.

Quando o peso passa pelo eixo vertical (onde o deslocamento é zero) a velocidade está no máximo e isso é traçado no diagrama de fase em B. Em C, quando o peso está na outra extremidade da oscilação, o deslocamento é negativo e a velocidade é zero. O peso então oscila de volta através de D (onde está indo na direção oposta, de maneira que sua velocidade é negativa) e completa uma oscilação em E.



No diagrama de fase isso é representado por uma rotação de  $360^\circ$ , mas como a oscilação é reduzida o ponto E é mostrado *dentro* de A. À medida que o pêndulo vai oscilando cada vez menos e menos, essa fase retrata espirais na origem até que eventualmente o pêndulo chegue ao repouso.

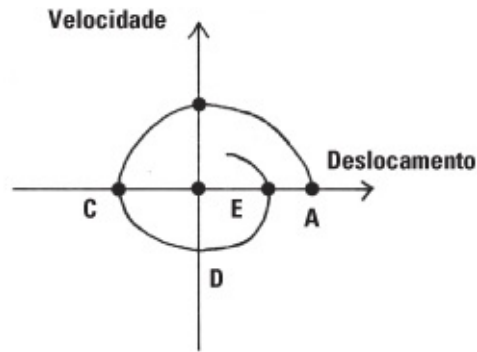
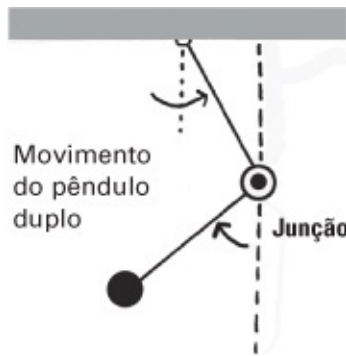


Diagrama de fase para o pêndulo simples

Esse não é o caso para o pêndulo duplo, no qual o peso está na extremidade de um par de bastões unidos. Se o deslocamento for pequeno, o movimento do pêndulo duplo é semelhante ao do pêndulo simples, mas se o deslocamento for grande, o peso oscila, roda e balança sem rumo, e o deslocamento em torno da união intermediária é aparentemente aleatório. Se o movimento não for forçado, o peso vai também chegar ao repouso, mas a curva que descreve o movimento está longe de ser a bem-comportada espiral do pêndulo simples.

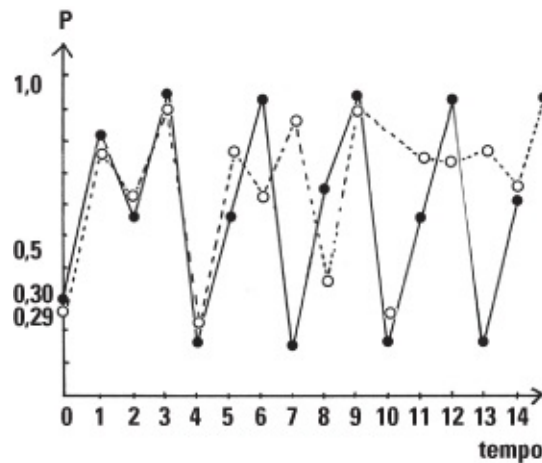
**Movimento caótico** A característica do caos é que um sistema determinístico pode parecer gerar comportamento aleatório. Vamos olhar outro exemplo, a fórmula repetitiva ou iterativa  $a \times p \times (1 - p)$  onde  $p$  quer dizer população, medida como uma proporção em uma escala de 0 a 1. O valor deve estar em algum lugar entre 0 e 4 para garantir que o valor de  $p$  esteja na faixa de 0 a 1.



Movimento do pêndulo duplo

Vamos modelar a população quando  $a = 2$ . Se pegarmos um valor inicial de, digamos,  $p = 0,3$  no *tempo* = 0, então, para encontrar a população no *tempo* = 1, nós incluímos  $p = 0,3$  em  $a \times p \times (1 - p)$  para obtermos 0,42. Usando não mais do que uma calculadora de mão, é possível repetir essa operação, dessa vez com  $p = 0,42$ , o que nos dará o número seguinte (0,4872). Progredindo desse jeito, encontramos a população em tempos posteriores. Nesse caso, a população rapidamente se estabiliza em  $p = 0,5$ . Essa estabilização sempre se dá para valores de  $a$  menores do que 3.

Se agora escolhermos  $a = 3,9$ , um valor próximo ao máximo permissível, e usarmos a mesma população inicial  $p = 0,3$  a população não se estabiliza, mas oscila descontroladamente. Isso é porque o valor de  $a$  está na “região caótica”, ou seja,  $a$  é um número maior do que 3,57. Além do mais, se escolhermos uma população inicial diferente,  $p = 0,29$ , um valor próximo a 0,3, o crescimento da população obscurece o padrão de crescimento anterior durante os primeiros passos, mas depois começa a divergir dele inteiramente. Esse é o comportamento experimentado por Edward Lorenz em 1961 (ver ao lado).



Mudança da população ao longo do tempo para  $\alpha = 3,9$ .

**Previsão do tempo** Mesmo tendo computadores potentes, todos nós sabemos que não conseguimos prever o tempo com mais de alguns dias de antecedência. Em apenas poucos dias de previsão, o tempo ainda nos faz surpresas desagradáveis. Isso acontece porque as equações que governam o tempo são não lineares – elas envolvem variáveis multiplicadas umas pelas outras, não apenas as variáveis propriamente ditas.

## Da meteorologia à matemática

A descoberta do efeito borboleta ocorreu por acaso por volta de 1961. Quando o meteorologista Edward Lorenz, no MIT, foi pegar uma xícara de café e deixou seu antigo computador traçando gráficos, ele voltou e encontrou uma coisa inesperada. Ele tinha como meta a retomada de alguns gráficos de tempo interessantes, mas encontrou o novo gráfico irreconhecível. Isso era estranho, porque ele tinha dado entrada com os mesmos valores iniciais e devia ter resultado no desenho da mesma imagem. Será que estava na hora de trocar seu velho computador por alguma coisa mais confiável?

Depois de alguma reflexão ele notou uma diferença no modo como entrara com os valores iniciais: antes ele tinha usado seis casas decimais, mas na segunda vez só se incomodou em botar três. Para explicar a disparidade ele cunhou o termo “efeito borboleta”. Depois dessa descoberta seus interesses intelectuais migraram para a matemática.

A teoria por trás da matemática da previsão do tempo foi elaborada independentemente pelo engenheiro francês Claude Navier em 1821 e pelo matemático físico britânico George Gabriel Stokes em 1845. As equações de Navier–Stokes que resultaram são de grande interesse para os cientistas.

Embora se saiba muito a respeito da teoria de sistemas de equações lineares, as equações de Navier–Stokes contêm termos não lineares que as tornam intratáveis. Praticamente o único jeito de resolvê-las é numericamente, usando computadores poderosos.

**Atratores estranhos** Pode-se pensar que sistemas dinâmicos possuem “atratores” em seus diagramas de fase. No caso do pêndulo simples o atrator é o ponto singular na origem, em direção ao qual o movimento é dirigido. Com o pêndulo duplo, é mais complicado, mas mesmo aí a imagem de fase vai exibir alguma regularidade e vai ser atraída para um conjunto de pontos no diagrama de fase. Para sistemas como esse, o conjunto de pontos pode formar um fractal (ver p. 100) que é chamado de atrator “estranho”, e terá uma estrutura matemática definida. Então nem tudo está perdido. Na nova teoria do caos, o que resulta não é tanto o caos “caótico” quanto

o caos “regular”.

**A ideia condensada:  
a turbulência da  
regularidade**

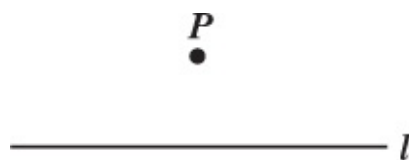


## 27 O postulado das paralelas

### linha do tempo

c.300 a.C.	1829-31	1854	1872	1915
Euclides inclui o postulado das paralelas em seu <i>Elementos</i>	Lobachevsky e Bolyai publicam seu trabalho sobre a geometria hiperbólica	Riemann dá palestras sobre os fundamentos de geometria	Klein unifica a geometria pela teoria dos grupos	A teoria da relatividade geral de Einstein é baseada na geometria riemanniana

Essa história impressionante começa com um simples cenário geométrico. Imagine uma linha  $l$  e um ponto  $P$  fora da linha. Quantas linhas podemos traçar através do ponto  $P$ , paralelas à linha  $l$ ? Parece evidente que há exatamente uma linha através de  $P$  que jamais vai encontrar  $l$  não importa o quanto seja estendida para qualquer direção. Isso parece autoevidente e em perfeito acordo com o bom senso. Euclides de Alexandria incluiu uma variante nesse postulado, nos fundamentos de geometria, os *Elementos*.



O quinto postulado de Euclides.

O bom senso não é sempre um guia confiável. Vamos ver se a suposição de Euclides faz sentido matemático.

**Os *Elementos* de Euclides** A geometria de Euclides é estabelecida nos 13 livros dos *Elementos*, escritos por volta de 300 a.C. Um dos textos mais influentes já escritos, era referido pelos matemáticos gregos como a primeira codificação sistemática da geometria. Sábios posteriores estudaram e traduziram a obra a partir de manuscritos sobreviventes, e ela foi passada adiante e

universalmente louvada como sendo o próprio modelo do que a geometria devia ser.

Os *Elementos* infiltraram-se até o nível escolar e a geometria era ensinada por meio de leituras do “livro sagrado”. Ela se provou inadequada para os alunos mais jovens, no entanto. Como o poeta A.C. Hilton satirizou: “embora escrevessem tudo de cor, não escreviam certo”. Você pode dizer que Euclides foi escrito para homens, não para meninos. A influência do livro nas escolas inglesas alcançou o apogeu como uma matéria no currículo durante o século XIX, mas permanece a pedra de toque para os matemáticos ainda hoje.

É o estilo dos *Elementos* de Euclides que o torna notável – sua proeza foi a apresentação da geometria como uma sequência de proposições provadas.

Sherlock Holmes teria admirado seu sistema dedutivo que avançava logicamente a partir dos postulados claramente enunciados, e pode ter ralhado com o dr. Watson por não o perceber como um “sistema frio, sem emoção”.

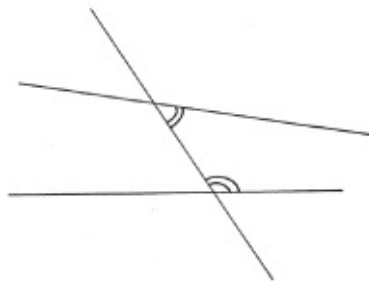
Embora o edifício da geometria de Euclides se baseie nos postulados (atualmente são chamados de axiomas; ver ao lado), esses não eram suficientes. Euclides acrescentou “definições” e “noções comuns”. As definições incluem declarações tais como “um ponto é o que não tem partes” e “uma linha é um comprimento sem largura”. Noções comuns incluem itens como “o todo é maior do que a parte” e “coisas que são iguais à mesma coisa são também iguais entre si”. Foi só lá pelo final do século XIX que se reconheceu que Euclides tinha feito suposições

tácitas.

## Os postulados de Euclides

Uma das características da matemática é que algumas poucas suposições podem gerar teorias amplas. Os postulados de Euclides são um excelente exemplo, e um exemplo que estabeleceu o modelo para sistemas axiomáticos posteriores. Seus cinco postulados são:

1. Uma linha reta pode ser traçada a partir de qualquer ponto para qualquer ponto.
2. Uma linha reta finita pode ser estendida continuamente em uma linha reta.
3. Um círculo pode ser construído com qualquer centro e qualquer raio.
4. Todos os ângulos retos são iguais uns aos outros.
5. Se uma linha reta que caia sobre duas linhas retas faz com que os ângulos interiores no mesmo lado sejam menores do que dois ângulos retos, as duas linhas retas, se estendidas indefinidamente, encontram-se naquele lado no qual os ângulos são menores do que dois ângulos retos.



**O quinto postulado** Foi o quinto postulado de Euclides que causou controvérsias mais de 2 mil anos depois de os *Elementos*

terem sido publicados pela primeira vez. Só o estilo já parece fora de lugar por sua prolixidade e falta de jeito. O próprio Euclides ficou infeliz com o trabalho, mas precisava dele para provar as proposições e teve de incluí-lo. Ele tentou prová-lo a partir de outros postulados, mas não conseguiu.

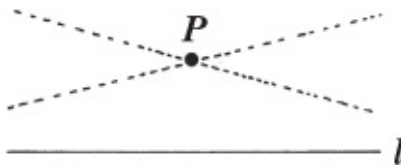
Matemáticos posteriores tentaram ou prová-lo ou substituí-lo por um postulado mais simples. Em 1795, John Playfair o enunciou em uma forma que ganhou popularidade: para uma linha  $l$  e um ponto  $P$  que não esteja na linha  $l$ , há uma única linha passando por  $P$  paralela a  $l$ . Por volta da mesma época, Adrien Marie Legendre substituiu isso por outra versão equivalente quando afirmou a existência de um triângulo cuja soma dos ângulos é  $180^\circ$ .

Essas novas formas do quinto postulado deram alguns passos na direção de satisfazer a objeção de artificialidade. Eles eram mais aceitáveis do que a incômoda versão dada por Euclides.

Outra linha de ataque era buscar a prova elusiva do quinto postulado. Isso exerceu uma poderosa atração sobre seus adeptos. Se uma prova pudesse ser encontrada, o postulado se tornaria um teorema e poderia se aposentar da linha de fogo. Infelizmente as tentativas nesse sentido acabaram sendo excelentes exemplos de raciocínio circular, argumentos que supõem exatamente a mesma coisa que eles estão tentando provar.

**Geometria não euclidiana** Um avanço veio pelos trabalhos de Carl Friedrich Gauss, János Bolyai e Nikolai Ivanovich Lobachevsky. Gauss não publicou seu trabalho, mas parece claro

que ele alcançou sua conclusão em 1817. Bolyai publicou o seu em 1831 e Lobachevsky, independentemente, em 1829, provocando uma discussão sobre prioridade entre esses dois. Não há dúvidas quanto ao brilhantismo de todos esses homens. Eles efetivamente mostraram que o quinto postulado era independente dos outros quatro postulados. Ao acrescentar sua negação aos outros quatro postulados, eles mostraram que um sistema consistente era possível.



Bolyai e Lobachevsky construíram uma nova geometria ao permitir que houvesse mais do que uma linha atravessando  $P$ , que não encontra a linha  $l$ . Como pode ser isso? Certamente as linhas pontilhadas encontram  $l$ . Se aceitarmos isso, estaremos inconscientemente caindo na visão de Euclides. O diagrama é, portanto, um truque de confiança, porque o que Bolyai e Lobachevsky estavam propondo era um novo tipo de geometria que não obedece à geometria do bom senso de Euclides. De fato, a geometria não euclidiana deles pode ser considerada como a geografia na superfície curva do que é conhecido como uma pseudoesfera.

Os caminhos mais curtos entre os pontos em uma pseudoesfera desempenham o mesmo papel que as linhas retas na geometria de Euclides. Uma das curiosidades dessa geometria não euclidiana é que a soma dos ângulos em um triângulo é menor do que  $180^\circ$ . Essa geometria é chamada de geometria

hiperbólica.



Outra alternativa ao quinto postulado formula que cada linha que passe por  $P$  se encontra com a linha  $l$ . Dito de outra forma, não há qualquer linha através de  $P$  que seja “paralela” a  $l$ . Essa geometria é diferente da de Bolyai e Lobachevsky, mas mesmo assim é uma geometria legítima.

Um modelo para ela é a geometria na superfície de uma esfera. Aqui os grandes círculos (aqueles círculos que têm a mesma circunferência que a própria esfera) desempenham o papel das linhas retas na geometria euclidiana. Nessa geometria não euclidiana, a soma dos ângulos de um triângulo é maior do que  $180^\circ$ . Ela é chamada de geometria elíptica e é associada ao matemático alemão Bernhard Riemann, que a investigou nos anos 1850.

A geometria de Euclides, que sempre foi considerada a verdadeira geometria – de acordo com Immanuel Kant, a geometria “inata ao homem” –, foi derrubada de seu pedestal. A geometria de Euclides é agora uma entre muitos sistemas, ensanduichada entre a geometria hiperbólica e a geometria elíptica. As diferentes versões foram unificadas sob uma só

cobertura por Felix Klein em 1872. O advento da geometria não euclidiana foi um evento de terremoto na matemática, e preparou o terreno para a geometria da relatividade geral de Einstein (ver p. 194). É a teoria *geral* da relatividade que exige um novo tipo de geometria – a geometria curva do espaço-tempo, ou geometria riemanniana. Foi essa geometria não euclidiana que passou a explicar porque as coisas caem, e não a força gravitacional atrativa entre objetos de Newton. A presença de coisas maciças no espaço, como a Terra e o Sol, faz com que o espaço-tempo seja curvo. Uma bola de gude em uma folha de borracha fina vai provocar um pequeno amassado, mas tente botar uma bola de boliche sobre ela e o resultado será um grande empenamento.

Essa curvatura medida pela geometria riemanniana prevê como os feixes de luz se encurvam na presença de objetos maciços no espaço. O espaço euclidiano comum, tendo o tempo como componente independente, não é suficiente para a relatividade geral. Um dos motivos é porque o espaço euclidiano é plano – não há curvatura. Pense em uma folha de papel em cima de uma mesa; podemos dizer que em qualquer ponto no papel a curvatura é zero. Subjacente ao espaço-tempo riemanniano está um conceito de curvatura que varia de maneira contínua – exatamente como a curvatura de um pedaço de pano amarrotado varia de ponto a ponto. É como olhar em um espelho deformador de parque de diversões – a imagem que você vê depende de onde você olhe no espelho.

Não é de admirar que Gauss ficasse tão impressionado com o jovem Riemann nos anos 1850, e até sugerisse na época que a

“metafísica” do espaço iria ser revolucionada pela percepção dele.

**A ideia condensada:  
e se as linhas paralelas  
se encontrarem?**



## 28 Geometria discreta

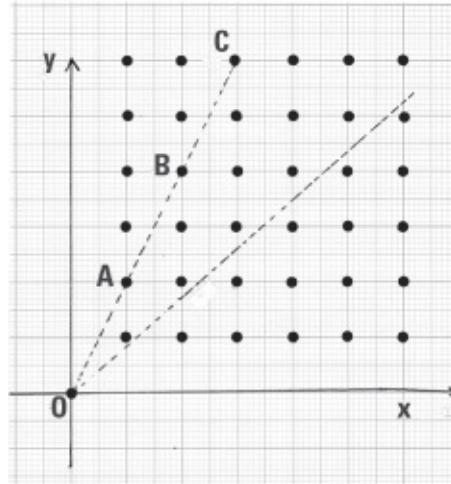
### linha do tempo

1639 d.C.	1806	1846	1892	1899
Pascal descobre seu teorema quando tinha apenas 16 anos de idade	Brianchon descobre o teorema dual de Pascal	Kirkman prevê a descoberta dos Sistemas Triplos de Steiner	Fano descobre o plano de Fano, o exemplo mais simples de uma geometria projetiva	Pick publica seu teorema sobre a área de polígonos

**Geometria é uma das artes mais antigas – ela literalmente significa medida (metri) da terra (geo). Na geometria comum há linhas contínuas e formatos sólidos para investigar, e os dois podem ser considerados como sendo compostos por pontos “próximos” uns dos outros. A matemática discreta lida com números inteiros, em oposição aos números reais contínuos. A geometria discreta pode envolver um número finito de pontos e linhas ou grades de pontos – o contínuo é substituído pelo isolado.**

Uma treliça, ou grade, é normalmente o conjunto dos pontos cujas coordenadas são números inteiros. Essa geometria apresenta problemas interessantes e tem aplicações em áreas tão díspares quanto teoria dos códigos e o projeto de experiências científicas.

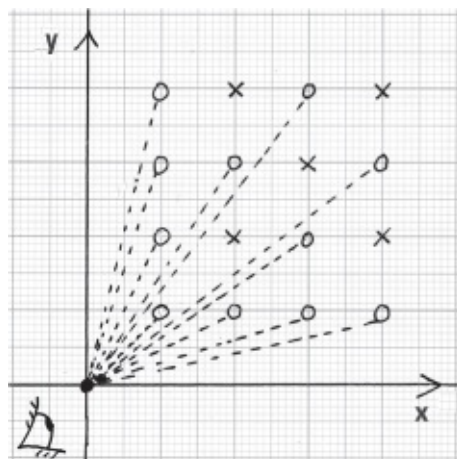
Vamos olhar para um farol que emite um fecho de luz. Imagine que o raio de luz começa na origem  $O$  e passa entre a horizontal e a vertical. Podemos perguntar que raios atingem que pontos da treliça (que podem ser barcos amarrados no porto em um arranjo um tanto uniforme).

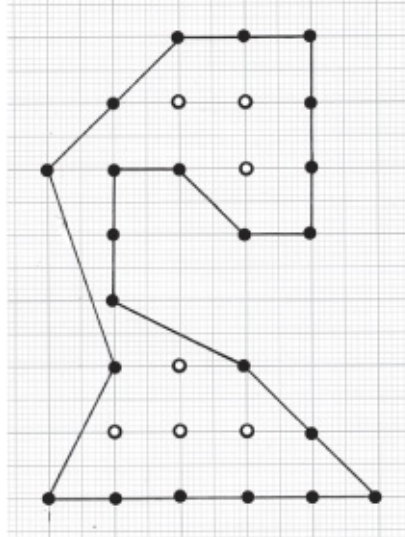


Os pontos da grade dos eixos  $x/y$

A equação do raio através da origem é  $y = mx$ . Essa é a equação de uma linha reta passando pela origem com gradiente  $m$ . Se o raio é  $y = 2x$ , então ele vai atingir o ponto com coordenadas  $x = 1$  e  $y = 2$  porque esses valores satisfazem a equação. Se o raio atingir um ponto na grade com  $x = a$  e  $y = b$ , o gradiente  $m$  é a fração  $b/a$ . Consequentemente, se  $m$  não for uma fração legítima (pode ser  $\sqrt{2}$ , por exemplo), o raio de luz não vai acertar nenhum ponto na grade.

O raio de luz  $y = 2x$  acerta o ponto A com coordenadas  $x = 1$  e  $y = 2$ , mas não vai acertar o ponto B, que tem coordenadas  $x = 2$  e  $y = 4$ , e todos os demais pontos “atrás” de A (como C, com coordenadas  $x = 3$  e  $y = 6$ , e D com  $x = 4$  e  $y = 8$ ) ficarão no escuro.





Um formato de muitos lados, ou poligonal

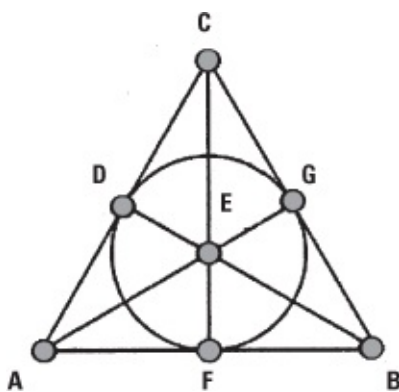
Para encontrar a área do formato, teremos de contar o número de pontos • no contorno e o número de pontos interiores o. No nosso exemplo, o número de pontos no contorno é  $b = 22$  e o número de pontos interiores é  $c = 7$ . Isso é tudo de que precisamos para usar o teorema de Pick:

$$\text{Área} = b/2 + c - 1$$

A partir dessa fórmula, a área é  $22/2 + 7 - 1 = 17$ . A área tem 17 unidades quadradas. É simples assim. O teorema de Pick pode ser aplicado a qualquer formato que junte pontos discretos com coordenadas de números inteiros, e a única condição é que o contorno não se cruze a si próprio.

**O plano de Fano** A geometria do plano de Fano foi descoberta mais ou menos ao mesmo tempo que a fórmula de Pick, mas não tem nada a ver com a medição de qualquer coisa. Batizado em homenagem ao matemático italiano Gino Fano, pioneiro no estudo da geometria finita, o plano de Fano é o exemplo simples

de uma geometria “projetiva”. Tem apenas sete pontos e sete linhas.



## O plano de Fano

Os sete pontos foram chamados de  $A, B, C, D, E, F$  e  $G$ . É fácil escolher seis linhas em sete, mas onde está a sétima? As propriedades da geometria e o modo pelo qual o diagrama é construído tornam necessário tratar a sétima linha como  $DFG$  – o círculo que passa por  $D, F$  e  $G$ . Isso não é problema, já que as linhas na geometria discreta não têm de ser “retas” no sentido convencional.

Essa pequena geometria tem diversas propriedades, por exemplo:

- Cada par de pontos determina uma linha que passa pelos dois.
- Cada par de linhas determina um ponto que está presente nas duas.

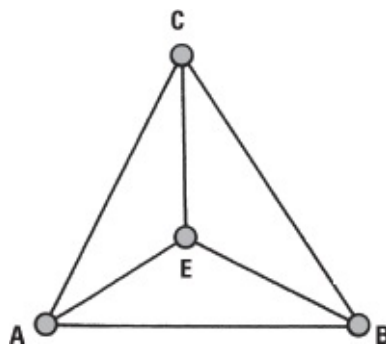
Essas duas propriedades ilustram a notável dualidade que ocorre nas geometrias desse tipo. A segunda propriedade é apenas a primeira com as palavras “ponto” e “linha” trocados, e do mesmo modo, a primeira é apenas a segunda com as mesmas trocas.

Se, em qualquer afirmação verdadeira, trocarmos as duas palavras e fizermos pequenos ajustes para corrigir a linguagem, obteremos outra declaração verdadeira. A geometria projetiva é muito simétrica. A geometria euclidiana, nem tanto. Na geometria euclidiana há linhas paralelas, ou seja, pares de linhas que nunca se encontram. Podemos muito alegremente falar do conceito de paralelismo na geometria euclidiana. Isso não é possível na geometria projetiva. Nela, todos os pares de linhas se

encontram em um ponto. Para os matemáticos isso significa que a geometria euclidiana é um tipo inferior de geometria.

Se retirarmos uma linha e seus pontos do plano de Fano, estaremos mais uma vez de volta ao reino da geometria euclidiana assimétrica e da existência de linhas paralelas. Vamos supor que retiramos a linha “circular”  $DFG$  para produzir um diagrama euclidiano.

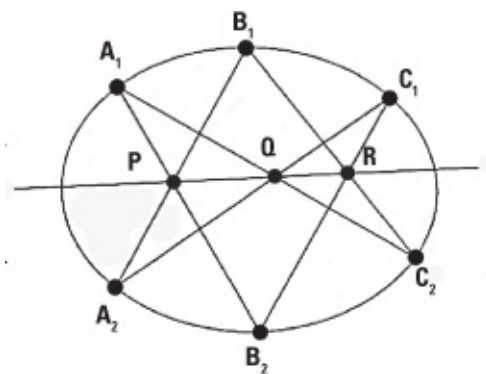
Com uma linha a menos agora são seis linhas:  $AB$ ,  $AC$ ,  $AE$ ,  $BC$  e  $CE$ . Há agora pares de linhas que são “paralelas”, isso é,  $AB$  e  $CE$ ,  $AC$  e  $BE$ , e  $BC$  e  $AE$ . As linhas são paralelas nesse sentido se elas não tiverem pontos em comum – como as linhas  $AB$  e  $CE$ .



O plano de Fano tornado euclidiano

O plano de Fano ocupa uma posição icônica na matemática por causa de suas conexões com tantas ideias e aplicações. É uma chave para o problema da colegial, proposto por Thomas Kirkman (ver p. 169). Na teoria do projeto de experiências o plano de Fano aparece como um exemplo extremamente variável, um Sistema Triplo de Steiner (STS). Dado um número finito de  $n$  objetos, um STS é um modo de dividi-los em blocos de três, de modo que cada par tomado dos  $n$  objetos está em exatamente um bloco. Dados os sete objetos  $A, B, C, D, E, F$  e  $G$  os

blocos no STS correspondem às linhas no plano de Fano.





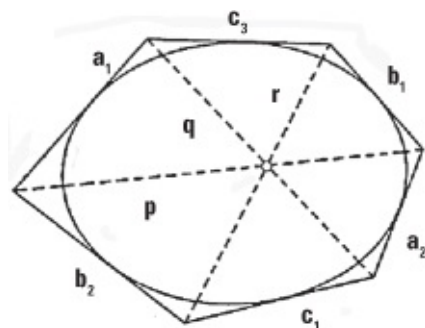
## Teorema de Pascal

**Um par de teoremas** O teorema de Pascal e o teorema de Brianchon ficam na divisa entre a geometria contínua e a geometria discreta. Elas são diferentes, mas relacionadas. O teorema de Pascal foi descoberto por Blais e Pascal em 1639, quando ele tinha apenas 15 anos. Vamos tomar um círculo esticado, chamado de elipse (ver p. 91) e marcar seis pontos ao longo dela, que vamos chamar de  $A_1, B_1$  e  $C_1$  e  $A_2, B_2$  e  $C_2$ . Vamos chamar de  $P$  o ponto em que a linha  $A_1B_2$  intersecta  $A_2B_1$ ;  $Q$  o ponto onde a linha  $A_1C_2$  intersecta  $A_2C_1$ ; e  $R$  o ponto em que a linha  $B_1C_2$  intersecta  $B_2C_1$ . O teorema declara que os pontos  $P, Q$  e  $R$  estão sobre uma única linha reta.

O teorema de Pascal é verdadeiro, não importando a posição dos diferentes pontos em torno da elipse. Na verdade, poderíamos substituir a elipse por uma cônica diferente, como a hipérbole, o círculo, parábola ou até um par de linhas retas (nesse caso a configuração é referida como “cama de gato”) e o teorema ainda assim seria verdadeiro.

O teorema de Brianchon foi descoberto muito mais tarde pelo matemático e químico francês Charles-Julie Brianchon. Vamos traçar seis tangentes, que chamaremos de linhas  $a_1, b_1$  e  $c_1$ , e  $a_2, b_2$  e  $c_2$ , que tocam a circunferência da elipse. Em seguida, podemos definir três diagonais, as linhas  $p, q$  e  $r$ , pelo encontro de linhas, de modo que:  $p$  é a linha entre os pontos onde  $a_1$  se encontra com  $b_2$  e em que  $a_2$  encontra  $b_1$ ;  $q$  é a linha entre os pontos em que  $a_1$  encontra  $c_2$  e  $a_2$  encontra  $b_1$ ; e  $r$  é a linha entre os pontos onde  $b_1$  encontra  $c_2$  e  $b_2$  encontra  $c_1$ . O teorema de

Brianchon enuncia que as linhas  $p$ ,  $q$  e  $r$  se encontram em um ponto.



## Teorema de Brianchon

Esses dois teoremas são duais entre si, e são outro exemplo dos teoremas da geometria projetiva ocorrendo em pares.

**A ideia condensada:  
pontos individuais  
de interesse**

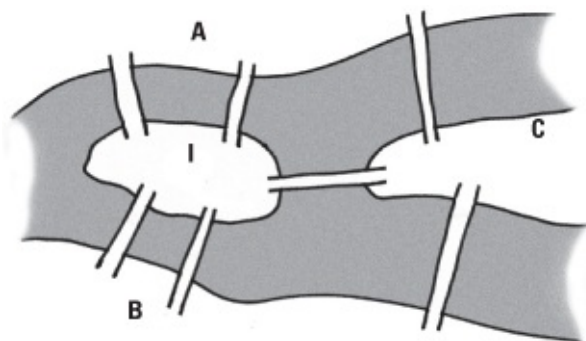
## 29 Grafos

### linha do tempo

1735 d.C.	1874	1930	1935	1999
Euler resolve o problema das pontes de Königsberg	Carl Schorlemmer liga a química com "árvores"	Kuratowski prova seu teorema de gráficos planares	George Pólya desenvolve técnicas de contagem para grafos como álgebra	Eric Rains e Neil Sloane estendem a contagem a árvores

**Há dois tipos de gráficos em matemática. Na escola, desenhamos curvas que mostram o relacionamento entre variáveis  $x$  e  $y$ . No outro tipo mais recente, os grafos, pontos são unidos por linhas sinuosas.**

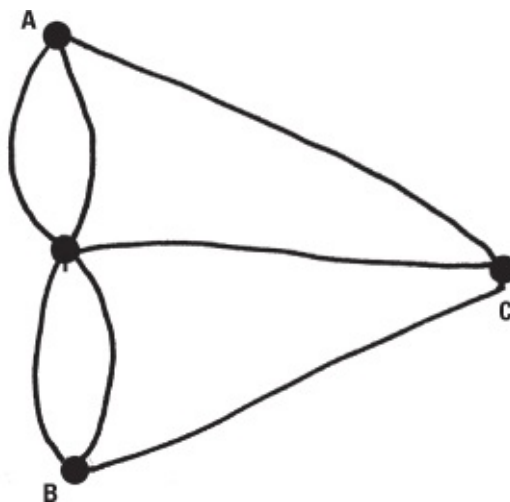
Königsberg é uma cidade na Prússia Oriental, famosa pelas sete pontes que cruzam o rio Pregel. Origem do ilustre filósofo Immanuel Kant, a cidade e suas pontes é ligada também ao famoso matemático Leonhard Euler.



No século XVIII, apresentou-se uma questão curiosa: seria possível sair e caminhar em torno de Königsberg atravessando cada ponte exatamente uma vez? A caminhada não tinha de acabar onde começara – só tinha de atravessar uma vez cada ponte.

Em 1735, Euler apresentou sua solução na Academia Russa, uma solução que é agora vista como o começo da moderna teoria dos

grafos. Em nosso diagrama semiabstrato, a ilha no meio do rio é chamada de *I* e as margens do rio são denominadas *A*, *B* e *C*. Será que você consegue planejar uma caminhada para uma tarde de domingo que atravessasse cada ponte apenas uma vez? Pegue um lápis e tente. O passo-chave é eliminar a semiabstração e ir para a abstração completa. Fazendo isso obtém-se um gráfico de pontos e linhas. A terra é representada por “pontos” e as pontes que os unem são representadas por “linhas”. Tanto faz se essas linhas não forem retas ou se tiverem comprimentos diferentes. Essas coisas não têm importância. A única coisa que importa são as conexões.

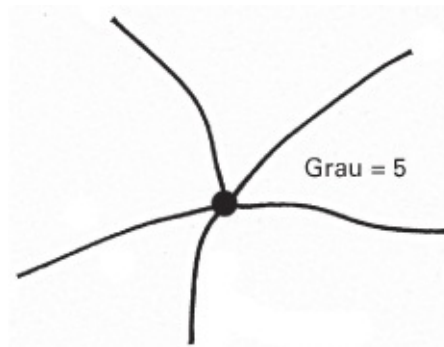


Euler fez uma observação a respeito de uma caminhada bem-sucedida. Fora o início e o fim da caminhada, cada vez que uma ponte é atravessada para uma porção de terra deve ser possível sair dela por uma ponte ainda não trilhada.

Traduzindo esse pensamento para a imagem abstrata, podemos dizer que as linhas que se encontram em um ponto devem ocorrer em pares. Fora dois pontos representando o início e o fim da caminhada, as pontes só podem ser atravessadas se, e

somente se, houver um par de linhas incidindo em cada ponto.

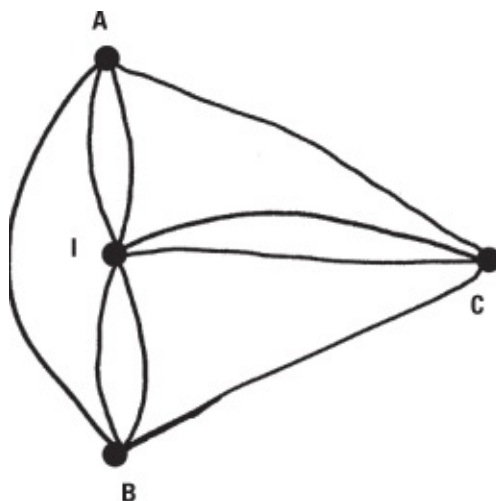
O número de linhas que se encontram em um ponto é chamado de “grau” do ponto.



O teorema de Euler enuncia que

*As pontes de uma cidade podem ser atravessadas exatamente uma vez se, fora no máximo dois, todos os pontos tiverem grau par.*

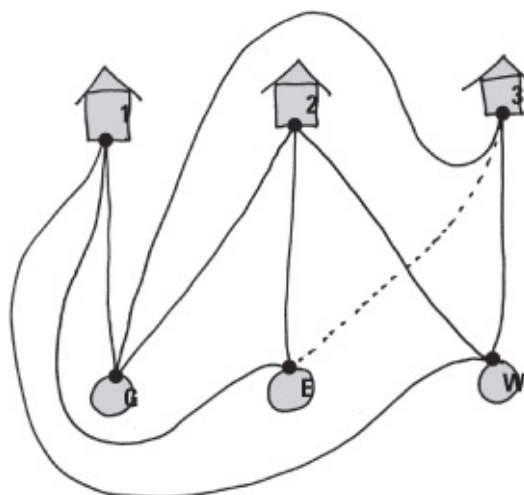
Se olharmos para o gráfico que representa Königsberg, cada ponto tem grau ímpar. Isso significa que uma caminhada atravessando cada ponte apenas uma vez não é possível em Königsberg. Se a disposição das pontes fosse mudada, então essa caminhada poderia se tornar possível. Se uma ponte a mais fosse construída entre a ilha *I* e *C* os graus em *I* e *C* seriam ambos pares. Isso significa que poderíamos começar uma caminhada em *A* e terminar em *B*, tendo passado por cada ponte exatamente uma vez. Se ainda outra ponte fosse construída, dessa vez entre *A* e *B* (mostrado à direita), poderíamos começar em qualquer lugar e terminar no mesmo lugar porque cada ponto nesse caso teria um grau par.



**O teorema do aperto de mão** Se nos pedissem para traçar um gráfico que contivesse três pontos de grau ímpar, teríamos um problema. Tente. Não pode ser feito.

*Em qualquer grafo, o número de pontos com grau ímpar tem de ser um número par.*

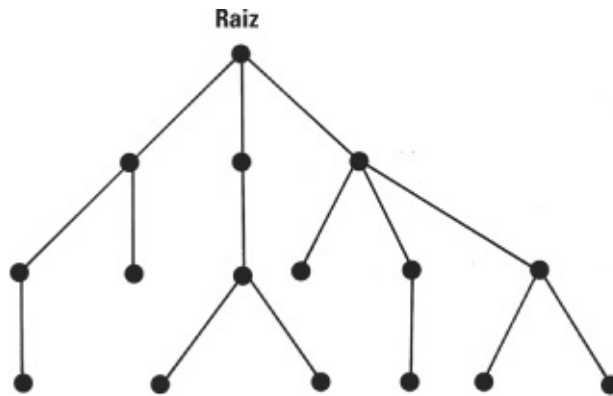
Esse é o teorema do aperto de mão – o primeiro teorema da teoria dos grafos. Em qualquer grafo, cada linha tem um começo e um fim; em outras palavras, é necessário que duas pessoas apertem as mãos. Se aumentarmos os graus de cada ponto para o grafo inteiro, teremos de obter um número par, digamos,  $N$ . Em seguida, dizemos que há  $x$  pontos com grau ímpar e  $y$  pontos com grau par. Somando todos os graus dos pontos ímpares, teremos  $N_x$  e somando todos os graus dos pontos pares teremos  $N_y$ , que é par. Então, temos  $N_x + N_y = N$ , portanto  $N_x = N - N_y$ . Daí se segue que  $N_x$  é par. Mas o próprio  $x$  não pode ser ímpar porque a soma de um número ímpar de graus ímpares seria um número ímpar, então segue-se que  $x$  tem de ser par.



**Grafos não planares** O problema dos serviços é um velho enigma. Imagine três casas e três serviços – gás, eletricidade e água. Temos de ligar cada uma das casas a cada um dos serviços, mas há um detalhe – as conexões não podem se cruzar.

Na verdade, isso não pode ser feito – mas você pode tentar com seus amigos confiantes. O grafo descrito ao se unir três pontos a outros três pontos de todos os modos possíveis (com apenas nove linhas) não pode ser traçado no plano sem que as linhas se cruzem. Tal grafo é chamado de não planar. Esse grafo dos serviços, junto ao feito por todas as linhas unindo cinco pontos, tem um lugar especial na teoria dos grafos. Em 1930, o matemático polonês Kazimierz Kuratowski provou o surpreendente teorema de que um grafo é planar se, e somente se, não contiver nenhum desses dois como subgrafo, um grafo menor contido dentro do grafo principal.

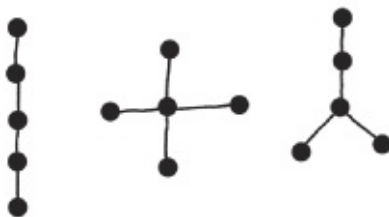




**Árvores** Uma “árvore” é um tipo particular de grafo, muito diferente do grafo dos serviços ou do de Königsberg. No problema das pontes em Königsberg havia oportunidade para começar em um ponto e voltar a ele por uma rota diferente. Essa rota que sai de um ponto e volta a ele mesmo é chamada de ciclo. Uma árvore é um grafo que não tem ciclos.

Um exemplo familiar de um grafo de árvore é o modo como os diretórios são arrumados em computadores. Eles são arranjados em uma hierarquia, com um diretório raiz dos quais saem subdiretórios. Como não há ciclos, não há como atravessar de um ramo a outro, a não ser através do diretório raiz – uma manobra familiar para os usuários de computadores.

**Árvores de números inteiros** Quantas árvores diferentes podem ser construídas a partir de um número específico de pontos? O problema das árvores de números inteiros foi abordado pelo matemático inglês do século XIX Arthur Cayley. Por exemplo, há exatamente três tipos diferentes de árvores com cinco pontos:



Cayley foi capaz de contar o número de diferentes tipos de árvores para números pequenos de pontos. Ele conseguiu chegar até árvores com menos de 14 pontos antes que a pura complexidade computacional se tornasse excessiva para um homem sem um computador. Desde então, o cálculo avançou para árvores com até 22 pontos. Há milhões de tipos possíveis para elas.

Até mesmo em sua própria época, a pesquisa de Cayley tinha aplicações práticas. Árvores de números inteiros são relevantes em química, em que a distinção entre alguns compostos depende do modo pelo qual os átomos estão dispostos em suas moléculas. Compostos com o mesmo número de átomos, mas arrumados de modo diferente, têm propriedades químicas diferentes. Com o uso de sua análise era possível prever a existência de substâncias químicas “na ponta do lápis” que depois eram descobertas no laboratório.

**A ideia condensada:  
cruzando pontes  
e subindo em árvores**

# 30 O problema das quatro cores

## linha do tempo

1852 d.C.	1879	1890	1976	1994
Guthrie, aluno de De Morgan, apresenta o problema a ele	Acredita-se que Kempe resolveu o problema	Heawood expõe erros na prova de Kempe e prova um teorema para cinco cores	Appel e Haken fornecem uma prova baseada em computador para o resultado geral	A prova do computador é simplificada, mas permanece sendo uma prova baseada em computador

**Quem poderia ter dado de presente de Natal ao pequeno Tim quatro lápis de cera coloridos e um mapa da Inglaterra em branco? Podia ter sido o vizinho cartógrafo que ocasionalmente enviava pequenos presentes, ou aquele matemático estranho, Augustus de Morgan, que morava perto e passava parte do dia com o pai de Tim. O senhor Scrooge é que não foi.**

**Os Cratchits moravam em uma desbotada casa geminada em Bayham Street, em Camden Town, logo ao norte do recém-aberto University College, onde De Morgan era professor. A origem do presente seria revelada no Ano Novo, quando o professor fez uma visita para ver se Tim tinha colorido o mapa.**

De Morgan tinha ideias definidas sobre como isso deveria ser feito: “Você tem de colorir o mapa de modo que duas regiões com uma fronteira comum tenham cores diferentes”.

“Mas eu não tenho cores em número suficiente”, disse Tim sem pensar. De Morgan teria sorrido e deixado o menino entregue à tarefa. Mas um de seus alunos, Frederick Guthrie, tinha há pouco lhe perguntado sobre esse problema, e mencionara ter conseguido colorir a Inglaterra com apenas duas cores. O problema mexeu com a imaginação matemática de De Morgan.

É possível colorir qualquer mapa com apenas quatro cores, de maneira que as regiões sejam diferenciadas? Cartógrafos podem ter acreditado que sim durante séculos, mas será que isso pode ser provado com rigor? Podemos pensar em qualquer mapa no mundo além do mapa municipal da Inglaterra, como os estados da América do Norte ou os departamentos franceses, e até mapas artificiais, feitos de regiões e fronteiras arbitrárias. Três cores, no entanto, não são suficientes.

Olhemos o mapa dos estados ocidentais dos Estados Unidos. Se tivéssemos apenas azul, verde e vermelho, poderíamos começar colorindo Nevada e Idaho. Não importa com que cores você começa, de modo que vamos escolher azul para Nevada e verde para Idaho. Até aqui, tudo bem. Essa escolha significaria que Utah *tem* de ser colorido de vermelho, e por sua vez, Arizona verde, Califórnia vermelho e Oregon verde. Isso significa que tanto Oregon quanto Idaho ficam verdes, de maneira que não os conseguimos distinguir. Mas se tivéssemos quatro cores, um amarelo também, poderíamos usar essa cor no Oregon e tudo estaria satisfatório. Será que essas quatro cores – azul, verde, vermelho e amarelo seriam suficientes para *qualquer* mapa? Essa questão é conhecida como o problema das quatro cores.



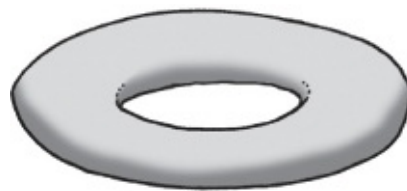
Os estados ocidentais dos Estados Unidos

**A disseminação do problema** Dentro de um período de 20 anos depois que De Morgan reconheceu que o problema tinha importância, ele se tornou conhecido dentro da comunidade matemática da Europa e da América. Nos anos 1860, Charles Sanders Peirce, um matemático e filósofo norte-americano, achou que tinha encontrado a prova, mas não há traços de seu argumento.

O problema ganhou maior notoriedade pela intervenção do homem de ciências vitoriano Francis Galton. Ele viu valor de publicidade no problema e induziu Arthur Cayley, eminente matemático de Cambridge, a escrever um artigo sobre o assunto em 1878. Infelizmente, Cayley foi obrigado a admitir que não tinha conseguido obter uma prova, mas observou que bastaria considerar apenas mapas cúbicos (em que exatamente três países se encontram em um ponto). A contribuição dele animou seu aluno Alfred Bray Kempe a tentar uma solução. Apenas um

ano mais tarde Kempe anunciou que tinha encontrado uma prova. Cayley agradeceu-o efusivamente, sua prova foi publicada e ele ganhou a eleição para a Royal Society de Londres.

**O que aconteceu em seguida?** A prova de Kempe era longa e tecnicamente exigente, e embora uma ou duas pessoas não ficassem convencidas com ela, foi geralmente aceita. Foi uma surpresa, dez anos mais tarde, quando Percy Heawood, baseado em Durham, encontrou um exemplo de mapa que expunha a falha no argumento de Kempe. Embora ele não conseguisse encontrar sua própria prova, Heawood mostrou que o desafio do problema das quatro cores ainda estava em aberto. Os matemáticos teriam de voltar para as pranchetas e alguns iniciantes teriam uma chance para se distinguirem. Usando algumas das técnicas de Kempe, Heawood provou um teorema de cinco cores – que qualquer mapa poderia ser colorido com cinco cores. Isso teria sido um grande resultado se alguém conseguisse construir um mapa que não pudesse ser colorido com quatro cores. Aí os matemáticos estavam em um dilema: era para ser quatro ou cinco cores?



A rosca simples, ou “torus”

O problema básico de quatro cores tratava de mapas desenhados em uma superfície plana ou esférica. E os mapas desenhados em uma superfície feito uma rosca – uma superfície mais

interessante para os matemáticos por causa de seu feitio do que pelo seu paladar. Para essa superfície, Heawood mostrou que sete cores eram tanto necessárias como suficientes para colorir qualquer mapa desenhado nela. Ele chegou a provar um resultado para uma rosca com múltiplos buracos (com  $h$  buracos), na qual ele contou o número de cores que garantiam que qualquer mapa podia ser colorido –, embora ele não tivesse provado que esse era o menor número de cores. Uma tabela para os primeiros poucos valores  $h$  de Heawood é: o número de buracos,  $h$  é:



Um “torus” com dois buracos

Número de buracos $h$	1	2	3	4	5	6	7	<u>8</u>
Número suficiente de cores, $C$	7	8	9	10	11	12	12	13

E, em geral,  $C = [1/2 (7 + \sqrt{1+48a})]$ . O colchete quadrado indica que tomamos apenas a parte inteira do termo dentro da equação. Por exemplo, quando  $h = 8$ ,  $c = [13,3107...] = 13$ . A fórmula de Headwood foi derivada da compreensão rigorosa de que o número de buracos é maior do que zero. A fórmula dá a torturante resposta  $c = 4$  se o valor  $h = 0$ , impedido, for substituído.

**Problema resolvido?** Depois de 50 anos, o problema que tinha aparecido em 1852 permanecia sem ter sido provado. No século XX, a capacidade mental dos matemáticos de elite no mundo

estava desconcertada.

Algum progresso foi feito, e um matemático provou que quatro cores eram suficientes para até 27 países em um mapa. Outro melhorou a marca, com 31 países, e um chegou a 35 países. Esse processo gradual, se continuasse, seria levado para sempre. Na verdade, as observações feitas por Kempe e Cayley em seus primeiros artigos forneceram um meio melhor de avanço, e matemáticos descobriram que tudo o que tinham a fazer era examinar algumas configurações de mapas para garantir que quatro cores bastassem. A questão era que há um grande número dessas configurações – nos estágios iniciais dessas tentativas para se obterem provas havia milhares de mapas a serem examinados. Esse exame não podia ser feito à mão, mas por sorte o matemático alemão Wolfgang Haken, que tinha trabalhado no problema durante muitos anos, foi capaz de recrutar os serviços do matemático norte-americano e especialista em computação Kenneth Appel. Métodos engenhosos reduziram o número de configurações a menos do que 1.500. Lá pelo fim de junho de 1976, depois de muitas noites sem dormir, a tarefa foi cumprida, e em parceria com seu fiel computador IBM 370, resolveram o grande problema.

O departamento de matemática da Universidade de Indiana tinha uma nova glória a trombetear. Eles substituíram seu selo postal “o maior número primo descoberto” pela notícia “quatro cores bastam”. Isso era orgulho local, mas onde estava o aplauso geral da comunidade matemática mundial? Depois de tudo, esse era um problema venerável que pode ser compreendido por qualquer pessoa com a pouca idade de pequeno Tim, mas que durante



bem mais de um século provocou e atormentou alguns dos maiores matemáticos.

O aplauso foi desigual. Alguns, muito a contragosto, aceitaram que a tarefa tinha sido cumprida, mas muitos permaneceram céticos. O problema era a prova ser com base em computador e isso saía inteiramente da forma tradicional de uma prova matemática. Era de se esperar que fosse ser difícil seguir uma prova, e que essa poderia ser uma prova longa, mas uma prova de computador era um passo grande demais. Levantava a questão de “verificabilidade”. Como poderia alguém verificar as milhares de linhas de código computacional da qual a prova depende? Certamente erros podem surgir na programação de computadores. Um erro pode ser fatal.

Isso não era tudo. O que estava realmente faltando era o fator “aha!”. Como poderia alguém ler a prova e apreciar a sutileza do problema, ou experimentar a parte crucial do argumento? Um dos críticos mais ferozes foi o eminente matemático Paul Halmos. Ele achou que uma prova de computador tinha tanta credibilidade quanto uma prova feita por um vidente de boa reputação. Mas muitos reconhecem essa realização, e só uma pessoa muito corajosa ou muito sem juízo gastaria seu precioso tempo de pesquisa tentando encontrar um contraexemplo de um mapa que exigisse cinco cores. Eles podem bem ter feito isso antes de Appel e Haken, mas não depois.

## A ideia condensada:



**quatro cores bastam**

# 31 Probabilidade

## linha do tempo

c.1650 d.C.	1785	1812	1912	1933
Os fundamentos da probabilidade são lançados por Pascal e Huygens	Condorcet aplica a probabilidade à análise de juris e sistemas eleitorais	Laplace publica seu livro de dois volumes <i>Teoria analítica da probabilidade</i>	Keynes publica seu <i>Tratado sobre a Probabilidade</i> , que influencia suas teorias sobre economia e estatística	Kolmogorov apresenta a probabilidade sob uma forma axiomática

**Qual é a chance de chover amanhã? Qual a probabilidade de eu pegar o trem mais cedo? Qual a probabilidade de você ganhar na loteria? Probabilidade, verossimilhança, chance, são todas palavras que usamos todos os dias quando queremos saber as respostas. São também palavras da teoria matemática da probabilidade.**

A teoria da probabilidade é importante. Ela tem uma relação com a incerteza e é um ingrediente essencial na avaliação de risco. Mas como uma teoria que envolve incerteza pode ser quantificada? Afinal, a matemática não é uma ciência exata?

O problema real é *quantificar* a probabilidade.

Suponha que tomemos o exemplo mais simples no planeta, atirar uma moeda. Qual é a probabilidade de dar cara? Podemos nos apressar e responder que é  $1/2$  (algumas vezes expressa como 0,5 ou 50%). Ao olhar para a moeda, fazemos a suposição de que é uma moeda honesta, o que quer dizer que a chance de ter cara é igual à chance de ter coroa, portanto a probabilidade de dar cara é  $1/2$ .

Situações que envolvem moedas, bolas e caixas e exemplos “mecânicos” são relativamente diretas. Há duas teorias

principais na atribuição de probabilidades. Olhar para a simetria de dois lados da moeda proporciona uma abordagem. Outra é a abordagem da frequência relativa, em que efetuamos a experiência um grande número de vezes e contamos o número de caras obtido. Mas quão grande é grande? É fácil acreditar que o número de caras relativo ao número de coroas é aproximadamente 50:50, mas pode ser que essa proporção mude, se continuarmos a experiência.

No entanto, e se chegamos a uma medida sensata da probabilidade de chover amanhã? Mais uma vez teremos dois resultados: ou chove ou não chove, mas não está de todo claro que eles sejam igualmente prováveis, como para a moeda.

Uma avaliação da probabilidade de chover amanhã terá de tomar em consideração as condições do tempo e uma multidão de outros fatores. Mas mesmo assim não é possível apontar o número exato para essa probabilidade. Embora possamos chegar a um número real, será útil atribuir um “grau de confiabilidade” de que a probabilidade será baixa, média ou alta. Em matemática, a probabilidade é medida em uma escala de 0 a 1. A probabilidade de um evento impossível é 0 e uma certeza é 1. Uma probabilidade de 0,1 significaria uma probabilidade baixa, enquanto 0,9 de probabilidade significaria uma probabilidade alta.

**Origens da probabilidade** A teoria matemática da probabilidade ganhou importância no século XVII com discussões sobre problemas de apostas entre Blaise Pascal, Pierre de Fermat e Antoine Gombaud (também conhecido como Chevalier de Méré).

Eles acharam um simples jogo intrigante. A questão do Chevalier de Méré é essa: o que é mais provável, rolar um “seis” em quatro jogadas de um dado ou rolar um “duplo seis” em 24 jogadas com dois dados? Em que opção você apostaria?

A sabedoria prevalecente na época achava que a melhor opção era apostar no seis duplo por permitir um maior número de jogadas. Essa opinião foi abaixo quando se analisaram as probabilidades. Eis aqui como são feitos os cálculos:

**Jogar um dado:** a probabilidade de não conseguir um seis com uma única jogada é  $5/6$ , e em quatro jogadas a probabilidade para isso seria  $5/6 \times 5/6 \times 5/6 \times 5/6$ , que é  $(5/6)^4$ . Como os resultados das jogadas não afetam umas às outras, elas são “independentes”, podemos multiplicar as probabilidades. A probabilidade de ter pelo menos um seis é então

$$1 - (5/6)^4 = 0,517746...$$

**Jogada de dois dados:** a probabilidade de não obter um seis duplo em uma jogada é  $35/36$  e em 24 jogadas essa probabilidade é  $(35/36)^{24}$ .

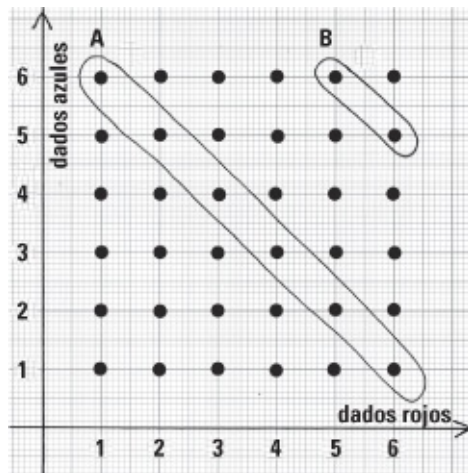
A probabilidade de pelo menos um seis duplo é, portanto,

$$1 - (35/36)^{24} = 0,491494...$$

Pode-se levar esse exemplo um pouco mais longe.

**Jogando dados (*craps*)** Os dois exemplos de dados é a base do jogo de dados moderno (*craps*) jogado em cassinos e em apostas on-line. Quando dois dados que podem ser distinguidos

(vermelho e azul) são jogados há 36 resultados possíveis, e esses resultados podem ser registrados como pares  $(x, y)$  e exibidos como 36 pontos contra um conjunto de eixos  $x/y$  – isso é chamado de “espaço da amostra”.



Espaço de amostra (para 2 dados)

Vamos considerar como “evento”  $A$  conseguir que a soma dos dados seja até 7. Há 6 combinações resultando, cada uma em 7, de modo que podemos descrever o evento como

$$A = \{(1,6), (2,5), (3,4), (4,3), (5,2), (6,1)\}$$

e os cercamos no diagrama. A probabilidade de  $A$  é de 6 chances em 36, que pode ser escrita como  $\Pr(A) = 6/36 = 1/6$ . Se fizermos  $B$  ser o evento em que se vai obter a soma dos dados igual a 11, temos que o evento  $B = \{(5,6), (6,5)\}$  e  $\Pr(B) = 2/36 = 1/18$ .

No jogo de *craps*, no qual dois dados são jogados em uma mesa, você pode ganhar ou perder no primeiro estágio, mas para alguns pontos nem tudo está perdido e você pode continuar para um segundo estágio. Você ganha na primeira jogada se ocorre ou o evento  $A$  ou o evento  $B$  – isso é chamado um “natural”. A

probabilidade de um natural é obtida somando-se as probabilidades individuais,  $6/36 + 2/36 = 8/36$ . Você perde no primeiro estágio se joga um 2, 3 ou um 12 (isso é chamado de *craps*). Um cálculo como esse acima dá a probabilidade de perder no primeiro estágio como sendo  $4/36$ . Se uma soma de 4, 5, 6, 8, 9 ou 10 é jogada, você vai para um segundo estágio e a probabilidade de isso acontecer é  $24/36 = 2/3$ .

No mundo dos jogos nos cassinos as probabilidades são escritas como chances. No jogo de *craps*, para cada 36 jogos que você jogue, em média você irá ganhar na primeira rodada 8 vezes e não ganhar 28 vezes, de modo que as chances contra ganhar na primeira rodada são 28 para 8, que é a mesma coisa que 3,5 para 1.

**O macaco na máquina de escrever** Alfred é um macaco que mora no zoológico local. Ele tem uma velha e castigada máquina de escrever, com 26 teclas para as letras do alfabeto, uma tecla para o ponto, uma para vírgula, uma para ponto de interrogação e uma para espaço – 30 teclas no total. Ele se senta a um canto, cheio de ambição literária, mas seu método de escrita é curioso – ele aperta as teclas aleatoriamente.

Qualquer sequência de letras digitadas terá uma chance não zero de ocorrer, de modo que há uma chance de ele digitar cada palavra das peças de Shakespeare. Mais do que isso, há uma chance (embora pequena) de ele seguir esse feito com uma tradução para o francês, depois para o espanhol e, em seguida, para o alemão. Para garantir, podemos permitir a possibilidade de ele continuar com os poemas de William Wordsworth. A



chance de isso tudo acontecer é minúscula, mas certamente não é zero. Esse é o ponto-chave.

Vamos ver quanto tempo ele gastará para digitar o solilóquio de *Hamlet* começando com a abertura “*To be or*”. Imaginamos 8 boxes que vão conter as 8 letras, incluindo os espaços.

T	o		b	e		o	r
---	---	--	---	---	--	---	---

O número de possibilidades para a primeira posição é 30, para a segunda é 30, e daí por diante. Então, o número de modos de preencher os boxes é  $30 \times 30 \times 30 \times 30 \times 30 \times 30 \times 30 \times 30$ . A chance de Alfred chegar até “*To be or*” é uma chance em  $6,561 \times 10^{11}$ . Se Alfred bater na máquina de escrever uma vez a cada segundo, há uma expectativa de que ele tenha digitado “*To be or*” em cerca de 20 mil anos, e tenha se mostrado um primata especialmente longo vivo. Então, não prenda a respiração esperando pelo Shakespeare inteiro. Alfred produzirá bobagens como “xoh?yt?” durante muito tempo.

**Como é que a teoria se desenvolveu?** Quando se aplica a teoria da probabilidade, os resultados podem ser controversos, mas pelo menos a matemática é razoavelmente segura. Em 1933, Andrey Nikolaevich Kolmogorov foi útil em definir probabilidade em bases axiomáticas – de maneira semelhante àquela pela qual os princípios da geometria foram definidos dois mil anos antes.

A probabilidade é definida pelos seguintes axiomas:

1. A probabilidade de todas as ocorrências é 1.
2. A probabilidade tem um valor maior ou igual a zero.

3. Quando ocorrências não podem coincidir, suas probabilidades podem ser somadas.

A partir desses axiomas, revestidos de linguagem técnica, as propriedades matemáticas da probabilidade podem ser deduzidas. O conceito de probabilidade pode ser amplamente aplicado. Grande parte da vida moderna não pode passar sem ele. Análise de risco, esporte, sociologia, psicologia, projetos de engenharia, finanças e daí por diante – a lista é infinita. Quem pensaria que os problemas de jogo que deram o pontapé inicial a essas ideias no século XVII iriam gerar uma disciplina tão enorme? Quais eram as chances de isso acontecer?

## **A ideia condensada: o sistema secreto do jogador**

## 32 Teoria de Bayes

### linha do tempo

1763 d.C	1937	1950	Década de 1950	1992
É publicado o ensaio de Bayes sobre probabilidade	De Finetti defende a probabilidade subjetiva como uma alternativa à teoria da frequência	Jimmy Savage e Dennis Lindley lideram o movimento bayesiano moderno	O termo "bayesiano" é usado pela primeira vez	É fundada a Sociedade Internacional de Análise Bayesiana

**Os primeiros anos do reverendo Thomas Bayes são obscuros. Nascido no sudeste da Inglaterra, provavelmente em 1702, ele se tornou um ministro de religião não conformista, mas também ganhou nome como matemático e foi eleito para a Royal Society de Londres em 1742. Seu famoso *Ensaio para a solução de um problema na doutrina das chances* foi publicado em 1763, dois anos depois de sua morte. Dava a fórmula para se encontrar a probabilidade inversa, a probabilidade “do contrário” e ajudou a criar um conceito central à filosofia bayesiana – a probabilidade condicional.**

Thomas Bayes deu seu nome aos bayesianos, os adeptos a um tipo de estatística diferente dos estatísticos tradicionais, ou “frequentistas”. Os frequentistas adotam uma visão da probabilidade baseada em dados numéricos rígidos. As ideias dos bayesianos estão centradas na famosa fórmula de Bayes e no princípio de que graus subjetivos de crença podem ser tratados como uma probabilidade matemática.

**Probabilidade condicional** Imagine que o galante dr. Why tem a tarefa de diagnosticar sarampo em seus pacientes. O aparecimento de manchas é um indicador usado para a detecção, mas o diagnóstico não é direto. Um paciente pode ter sarampo

sem ter manchas, e alguns pacientes podem ter manchas sem ter sarampo. A probabilidade de que um paciente tenha manchas, dado que ele tenha sarampo, é uma probabilidade condicional. Os bayesianos usam uma linha vertical em suas fórmulas para significar “dado”, então escrevemos

$Prob(\text{um paciente tem manchas} \mid \text{o paciente tem sarampo})$

Isso significa a probabilidade de manchas em um paciente se ele tiver sarampo. O valor de  $prob(\text{o paciente tem manchas} \mid \text{o paciente tem sarampo})$  não é o mesmo que  $prob(\text{o paciente tem sarampo} \mid \text{o paciente tem manchas})$ . Em relação uma à outra, uma é a probabilidade da outra ao contrário. A fórmula de Bayes é a fórmula para calcular uma a partir da outra. O que os matemáticos mais gostam é de usar notação para representar coisas. Então, digamos que o evento de ter sarampo é  $M$  e o evento de ter manchas é  $S$ . o símbolo  $\sim S$  é o evento de um paciente *sem* manchas  $\hat{M}$  é o evento de ele *não* ter sarampo. Podemos ver isso em uma tabela de entrada dupla.

	$S$	$\tilde{S}$	
$M$	$x$		$m$
$\tilde{M}$			$N$

Tabela com duas entradas mostrando a estrutura lógica da aparição das manchas e do sarampo

Isso diz ao dr. Why que há  $x$  pacientes que têm sarampo e manchas,  $m$  pacientes que têm sarampo, enquanto o número total de pacientes no geral é  $N$ . A partir do diagrama é possível

ver que a probabilidade de que alguns tenham sarampo e manchas é simplesmente  $x/N$ , enquanto a probabilidade de que alguém tenha sarampo é  $m/N$ . A probabilidade condicional, a probabilidade de que alguém tenha manchas, dado que ela tem sarampo, escrita  $prob(S \mid M)$  é  $x/m$ . Juntando isso tudo, o dr. Why obtém a probabilidade de que alguém tenha tanto sarampo como manchas.

$$Prob(M \& S) = \frac{x}{N} = \frac{x}{m} \times \frac{m}{N}$$

Ou

$$\textit{prob}(\text{M \& S}) = \textit{prob} (\text{S} \mid \text{M}) \times \textit{prob}(\text{M})$$

do mesmo jeito

$$prob(M \& S) = prob(M | S) \times prob(S)$$

**Fórmula de Bayes** Equacionando as expressões para  $prob(M \& S)$  temos a fórmula de Bayes, a relação entre a probabilidade condicional e o seu inverso. O dr. Why terá uma boa ideia a respeito de  $prob(S | M)$ , a probabilidade de que se um paciente tiver sarampo ele tenha manchas. É na probabilidade condicional do contrário que o dr. Why está realmente interessado, sua estimativa de que, se um paciente tiver manchas, ele terá sarampo. Descobrir isso é o problema inverso e o tipo de problema abordado por Bayes em seu artigo. Para calcular as probabilidades, precisamos acrescentar alguns números. Esses serão subjetivos, mas o que é importante é ver como eles se combinam. Se um paciente tem sarampo, a probabilidade de ele ter manchas será alta, digamos,  $prob(S|M) = 0,9$ , mas se ele não tem sarampo a probabilidade de manchas será baixa, digamos  $prob(S| \sim M)=0,15$ . O deslumbrante doutor terá também uma ideia a respeito da porcentagem de pessoas na população que têm sarampo, digamos, 20%. Isso é expresso como  $prob(M)= 0,2$ . A única outra informação de que precisamos é  $prob(S)$ , a porcentagem de pessoas na população que têm manchas. Agora a probabilidade de alguém ter manchas é a probabilidade de alguém ter sarampo e manchas mais a probabilidade de alguém não ter sarampo, mas ter manchas. Das nossas relações básicas,  $prob(S) = 0,9 \times 0,2 + 0,15 \times 0,8 = 0,3$ . Substituindo esses valores na fórmula de Bayes, dá:

$$prob(M | S) = \frac{0,2}{0,3} \times 0,9 = 0,6$$

$$prob(M|S) = \frac{prob(M)}{prob(S)} \times prob(S|M)$$

Fórmula de Bayes

A conclusão é que, de todos os pacientes com manchas que o doutor examina, ele detecta corretamente sarampo em 60% desses casos. Suponhamos agora que o médico recebe mais informações sobre o surto de sarampo, de modo que a probabilidade de detecção suba, ou seja,  $prob(S|M)$ , a probabilidade de ter manchas por causa do sarampo, aumente de 0,9 para 0,95 e  $prob(S|\sim M)$ , a probabilidade de manchas por outra causa, decaia de 0,15 para 0,1. Como essa mudança melhora sua taxa de detecção de sarampo? Qual é o novo  $prob(M|S)$ ? Com essa nova informação,  $prob(S) = 0,95 \times 0,2 + 0,1 \times 0,8 = 0,27$ , então, na fórmula de Bayes,  $prob(M|S)$  é 0,2 dividido por  $prob(S) = 0,27$  e então multiplicado por 0,95, que dá 0,704. Desse modo, o dr. Why agora consegue detectar 70% dos casos ao receber essa informação melhorada. Se as probabilidades mudarem para 0,99 e 0,01, respectivamente, então a probabilidade de detecção  $prob(M|S)$  passaria a ser 0,961, de maneira que sua chance de um diagnóstico correto nesse caso seria de 96%.

**Bayesianos atuais** O estatístico tradicional teria poucas objeções ao uso da fórmula de Bayes onde a probabilidade possa ser medida. O ponto de controvérsia é na interpretação da probabilidade com graus de convicção, ou, como é algumas vezes definida, a probabilidade subjetiva.



O “ônus da prova” em um tribunal está entre o “além da dúvida razoável” e o “no equilíbrio das probabilidades”. O primeiro critério é tradicionalmente aplicado em casos criminais, mas se o último viesse a ser aplicado para decidir quem é culpado ou inocente, seria muito importante saber como essas probabilidades seriam manejadas. Aqui entra em cena a análise bayesiana, e imaginamos um possível cenário ambientado em um caso criminal.

Um jurado acabou de ouvir um caso e decidiu que a probabilidade de o acusado ser culpado é cerca de 1 em 100. Durante as deliberações na sala do júri, o júri é chamado de volta ao tribunal para ouvir novas provas do promotor. Uma arma foi achada na casa do prisioneiro, e o principal promotor alega que a probabilidade de encontrá-la, se o prisioneiro for culpado, chega a ser de 0,95, mas se ele fosse inocente a probabilidade de encontrar a arma seria de apenas 0,1. A probabilidade de encontrar uma arma na casa do prisioneiro seria, portanto, muito mais alta se o prisioneiro for culpado do que se ele for inocente. A questão apresentada ao júri é: como deveriam eles mudar sua opinião sobre o prisioneiro à luz dessa nova informação? Usando outra vez a nossa notação,  $C$  é o evento em que o prisioneiro é culpado e  $P$  é o evento em que a nova prova é obtida. O júri tinha feito uma avaliação inicial de  $prob(C) = 1/100$  ou 0,01. Essa probabilidade é chamada de probabilidade anterior. A probabilidade reavaliada  $prob(C|P)$  é a probabilidade revista de culpa, dada pela nova prova,  $E$ , e essa é chamada de probabilidade posterior. A fórmula de Bayes sob a forma

$$\text{prob}(G | E) = \frac{\text{prob}(E | G)}{\text{prob}(E)} \times \text{prob}(G)$$

mostra a ideia da probabilidade anterior sendo atualizada para a probabilidade posterior  $prob(G|E)$ . Do mesmo modo que o cálculo da  $prob(S)$  no exemplo médico, podemos calcular  $prob(E)$  e vamos encontrar

$$prob(G | E) = \frac{0,95}{0,95 \times 0,01 + 0,1 \times 0,99} \times 0,01 = 0,088$$

Isso vai criar um dilema para o júri, porque a avaliação inicial de 1% de chance de culpa subiu para quase 9%. Se a acusação tivesse feito a alegação mais pesada, de que a probabilidade de encontrar a arma incriminadora chegaria a 0,99 se o prisioneiro fosse culpado, mas a probabilidade de encontrar a arma seria de apenas 0,01 se o prisioneiro fosse inocente, então, repetindo o cálculo da fórmula de Bayes, o júri teria de rever a opinião deles de 1% para 50%.

O uso da fórmula de Bayes nessas situações foi exposto a críticas. O ponto principal tem sido em como se define a probabilidade anterior. A análise bayesiana apresenta em seu favor um modo de lidar com as probabilidades subjetivas e como elas podem ser atualizadas com bases em evidências. O método bayesiano tem aplicações em áreas tão diversas quanto ciência, previsão do tempo e justiça criminal. Seus proponentes demonstram sua solidez e característica pragmática quando se lida com a incerteza. Há muita coisa a seu favor.

**A ideia condensada:  
atualização de crenças,  
uso de provas**

# 33 O problema do aniversário

## linha do tempo

1654 d.C.	1657	1718	Década de 1920	1939
Blaise Pascal lança os fundamentos da teoria das probabilidades	Christiaan Huygens escreve o primeiro trabalho publicado sobre probabilidade	Abraham de Moivre publica A doutrina do acaso, seguido de edições ampliadas em 1738 e 1756	Bose considera a teoria da luz de Einstein como um problema de ocupação	Richard von Mises propõe o problema do aniversário

**Imagine que você esteja no andar de cima do ônibus de Clapham sem nada especial para fazer além de contar quantos outros passageiros vão para o trabalho de manhã cedo. Como é provável que todos os passageiros sejam independentes uns dos outros, podemos com segurança supor que eles tenham seus aniversários espalhados aleatoriamente ao longo do ano. Incluindo você, há apenas 23 passageiros a bordo. Não é muito, mas é o suficiente para alegar que há uma boa chance de dois passageiros celebrarem no mesmo dia. Dá para acreditar? Milhões não acreditam, mas é absolutamente verdade. Até mesmo um reconhecido especialista em probabilidade, William Feller, achou isso espantoso.**

O ônibus de Clapham é agora pequeno demais para as nossas necessidades, de maneira que retomamos o argumento em uma sala grande. Quantas pessoas precisam se reunir numa sala para que haja *certeza* de que duas pessoas compartilham o mesmo aniversário? Há 365 dias em um ano padrão (vamos desconsiderar os anos bissextos para simplificar as coisas), então, se houver 366 pessoas na sala, pelo menos um par *definitivamente* terá o mesmo aniversário. Não pode acontecer de todas as pessoas terem aniversários diferentes.

Esse é o princípio do pombo: se houver  $n + 1$  pombos ocupando  $n$  espaços, um espaço teria de conter mais de um pombo. Se houver 365 pessoas, não poderemos ter certeza de que haja um aniversário em comum porque os aniversários poderiam ser um em cada dia do ano. Entretanto, se você tomar 365 pessoas aleatoriamente, isso seria altamente improvável e a probabilidade de duas pessoas não terem o mesmo aniversário seria minúscula. Mesmo se houver apenas 50 pessoas na sala, há uma chance de 96,5% de duas pessoas compartilharem o mesmo aniversário.

Se o número de pessoas for reduzido ainda mais, a probabilidade de duas pessoas terem o mesmo aniversário se reduz. Notamos que 23 pessoas é o número para o qual a probabilidade mal seja maior do que  $1/2$  e para 22 pessoas a probabilidade de um aniversário compartilhado mal seja menor do que  $1/2$ . O número 23 é o valor crítico. Embora a resposta ao clássico problema do aniversário seja surpreendente, não é um paradoxo.

**Podemos provar?** Como podemos nos convencer? Vamos escolher uma pessoa ao acaso. A probabilidade de que outra pessoa tenha o mesmo aniversário que ela é  $1/365$ , e então a probabilidade de que essas duas pessoas não compartilhem o aniversário é um menos isso (ou  $364/365$ ). A probabilidade de que ainda outra pessoa escolhida aleatoriamente tenha o mesmo aniversário que as outras duas é  $2/365$ , então a probabilidade de que essa pessoa não tenha o mesmo aniversário que nenhuma das duas primeiras é um menos isso (ou  $363/365$ ). A probabilidade de nenhuma dessas três pessoas compartilharem o aniversário é a multiplicação dessas duas probabilidades, ou

$(364/365) \times (363/365)$ , que é 0,9918.

Continuar nessa linha de pensamento para 4, 5, 6... pessoas desenreda o paradoxo do problema do aniversário. Quando chegamos a 23 pessoas com nossa calculadora de bolso, obtemos a resposta 0,4927 como a probabilidade de que ninguém entre elas tenha o mesmo aniversário. A negação de “nenhuma delas com o mesmo aniversário” é “pelo menos duas pessoas têm o mesmo aniversário”, e a probabilidade disso é  $1 - 0,4927 = 0,5073$ , que mal é maior do que o crucial  $1/2$ .

Se  $n = 22$ , a probabilidade de duas pessoas terem o mesmo aniversário é 0,4747, que é menos do que  $1/2$ . A natureza aparentemente paradoxal do problema do aniversário é ligada à linguagem. O resultado do aniversário faz uma declaração a respeito de duas pessoas compartilhando um aniversário, mas não nos diz que duas pessoas elas são. Não sabemos onde a coincidência vai cair. Se o sr. Trevor Thomson, cujo aniversário é no dia 8 de março, estiver na sala, pode-se fazer uma pergunta diferente.

**Quantos aniversários coincidem com o do sr. Thomson?** Para essa questão o cálculo é diferente. A probabilidade de o sr. Thomson não compartilhar seu aniversário com outra pessoa é de  $364/365$ , de modo que a probabilidade de que ele não compartilhe o aniversário com nenhuma das outras  $n-1$  pessoas na sala é  $(364/365)^{n-1}$ . Portanto, a probabilidade de que o sr. Thomson compartilhe seu aniversário com alguém será um menos esse valor.

Se computarmos isso para  $n = 23$ , essa probabilidade é de apenas

0,061151, de modo que há uma chance de apenas 6% de que alguém mais faça anos no dia 8 de março, a mesma data de aniversário do sr. Thomson. Se aumentarmos o valor de  $n$ , essa probabilidade vai aumentar. Mas temos de ir até  $n = 254$  (que inclui o sr. Thomson na contagem) para que a probabilidade seja maior do que  $1/2$ . Para  $n = 254$ , o valor é 0,5005. Esse é o ponto de corte porque  $n = 253$  dará o valor de 0,4991, que é menos do que  $1/2$ . Terá de haver uma reunião de 254 pessoas na sala para a chance ser maior do que  $1/2$  de que o sr. Thomson tenha o mesmo aniversário que outra pessoa. Isso talvez esteja mais em sintonia com a nossa intuição do que a surpreendente solução do problema clássico do aniversário.

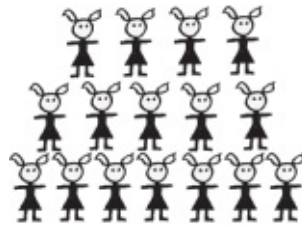
**Outros problemas de aniversário** O problema do aniversário tem sido generalizado de diversas maneiras. Uma abordagem é considerar três pessoas com o mesmo aniversário. Nesse caso, para que a chance de três pessoas terem o mesmo aniversário seja maior do que de 50%, seriam necessárias 88 pessoas. Há grupos correspondentemente maiores se quatro, cinco ou mais pessoas tiverem de partilhar o mesmo aniversário. Numa reunião de mil pessoas, por exemplo, há uma chance maior do que 50% de que nove delas tenham o mesmo aniversário.

Outras incursões no problema do aniversário indagaram sobre quase aniversários. Nesse problema uma combinação é considerada como tendo ocorrido se um aniversário estiver a uma distância de um determinado número de dias de outro aniversário. No fim, apenas 14 pessoas numa sala resultarão em uma chance maior do que 50% de duas pessoas terem um aniversário em comum, ou de terem o aniversário com um dia

de diferença uma da outra.

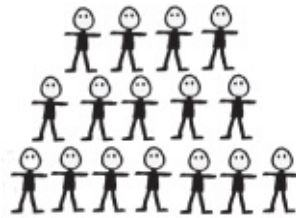
Uma variante do problema do aniversário que exige ferramentas matemáticas mais sofisticadas é o problema de meninos e meninas: se uma classe tem um número igual de meninos e meninas, qual seria o menor grupo a ter uma chance maior do que 50% de que um menino e uma menina tenham o mesmo aniversário?

O resultado é que o grupo mínimo seria uma classe de 32 (16 meninas e 16 garotos). Compare isso aos 23 do clássico problema do aniversário.





## Meninas



## Meninos

Mudando ligeiramente a questão, podemos obter outras novidades (mas elas não são fáceis de se responder). Suponhamos que haja uma longa fila se formando para um show de Bob Dylan e as pessoas entrem nessa fila aleatoriamente. Como estamos interessados em aniversários, podemos descontar a possibilidade de gêmeos ou trigêmeos chegarem juntos. À medida que os fãs entram, precisam informar seus aniversários. A questão matemática é essa: quantas pessoas você esperaria entrarem antes de duas pessoas *consecutivas* terem o mesmo aniversário? Outra questão: quantas pessoas entram no auditório antes que alguém surja com o mesmo aniversário que o sr. Trevor Thomson (8 de março)?

O cálculo do aniversário supõe que os aniversários estão uniformemente distribuídos e que cada aniversário tem a mesma chance de ocorrer para uma pessoa escolhida a esmo. Resultados experimentais mostram que isso não é exatamente verdadeiro (mais crianças nascem durante os meses de verão), mas é próximo o suficiente para que a solução seja aplicável.

Problemas de aniversário são exemplos de problemas de ocupação, em que os matemáticos pensam a respeito de colocar bolas em células. No problema do aniversário, o número de células é 365 (essas são identificadas com possíveis aniversários) e as bolas a serem colocadas aleatoriamente nas células são as pessoas. O problema pode ser simplificado para a investigação da probabilidade de duas bolas caírem na mesma célula. Para o problema meninos-e-meninas, as bolas são de duas cores.

Não são apenas os matemáticos que estão interessados no problema do aniversário. Satyendra Nath Bose era fascinado pela teoria da luz de Albert Einstein, baseada nos fótons. Ele saiu das linhas tradicionais de pesquisa e considerou a configuração física em termos de um problema de ocupação. Para ele, as células não eram dias do ano, como no problema do aniversário, mas níveis de energia dos fótons. Em vez de pessoas sendo postas em células, como no problema do aniversário, ele distribuiu números de fótons. Há muitas aplicações para problemas de ocupação em outras ciências. Na biologia, por exemplo, a disseminação de epidemias pode ser modelada como um problema de ocupação – as células nesse caso são áreas geográficas, as bolas as doenças e o problema é calcular como essas doenças se agrupam.

O mundo está cheio de coincidências assombrosas, mas só a matemática nos dá o meio de calcular a probabilidade de elas ocorrerem. O clássico problema do aniversário é apenas a ponta do iceberg com relação a isso, e é uma grande entrada para a matemática séria com aplicações importantes.

## **A ideia condensada: cálculo de coincidências**

# 34 Distribuições

## linha do tempo

1837 d.C.	1881	1898	1938	1950	2003
Siméon-Denis Poisson descreve a distribuição que leva seu nome	Newcomb descobre o que se torna conhecido como a lei de Benford	Bortkiewicz analisa as mortes dos cavaleiros da Prússia	Benford reafirma a lei da distribuição dos primeiros algarismos	Zipf deriva uma fórmula relacionando o uso de palavras a vocabulário	A distribuição de Poisson é usada para analisar quantos peixes havia no Atlântico Norte

**Ladislau J. Bortkiewicz era fascinado pelas tabelas de mortalidade. Para ele, esse não era um tema sombrio, e sim um campo de contínua investigação científica. É famosa a contagem que ele fez do número de cavaleiros no exército prussiano que morreram por causa de coices de cavalos. Depois houve Frank Benford, um engenheiro elétrico que contou os primeiros algarismos de diferentes tipos de dados numéricos para ver quantos eram uns, dois e daí por diante. E George Kingsley Zipf, que ensinava alemão em Harvard, tinha interesse em filologia e analisou a ocorrência de palavras em trechos de texto.**

Todos esses exemplos envolvem a medida da probabilidade de eventos. Quais são as probabilidades de  $x$  cavaleiros em um ano receberem um coice letal de um cavalo? Enumerar as probabilidades para cada valor de  $x$  é chamado de distribuição de probabilidades. É também uma distribuição discreta, porque os valores de  $x$  só adotam valores isolados – há falhas entre os valores de interesse. Você pode ter três ou quatro cavaleiros prussianos abatidos por um coice letal, mas não  $3\frac{1}{2}$ . Como veremos, no caso da distribuição de Benford só estamos interessados no aparecimento de dígitos 1, 2, 3,... e, para a distribuição de Zipf, você pode ter a palavra “isso” classificada

em oitavo lugar para as palavras principais, mas não na posição, digamos, 8,23.

**Vida e morte no exército prussiano** Bortkiewicz reuniu registros para dez batalhões ao longo de um período de 20 anos, obtendo dados para 200 anos-batalhão. Ele examinou o número de mortes (isso é o que os matemáticos chamam de variável) e o número de anos-batalhão durante os quais esse número de mortes ocorreu. Por exemplo, durante 109 anos-batalhão não ocorreu nenhuma morte, enquanto em um ano-batalhão houve quatro mortes. No quartel, digamos que o Batalhão C em um ano específico teve quatro mortes.

Com se distribui o número de mortes? Coletar essa informação é um aspecto do trabalho do estatístico – ir a campo e anotar resultados. Bortkiewicz obteve os seguintes dados:

Número de mortes	0	1	2	3	4
Frequência	109	65	22	3	1

Felizmente, morrer por coice de cavalo é um evento raro. A técnica teórica mais adequada para modelar a frequência de ocorrerem eventos raros é usar algo chamado de distribuição de Poisson. Com essa técnica, será que Bortkiewicz poderia ter previsto os resultados sem visitar as cocheiras? A distribuição teórica de Poisson diz que a probabilidade de que o número de mortes (que chamaremos de  $X$ ) tenha o valor  $x$  vem da fórmula de Poisson, onde  $e$  é o número especial discutido antes, e que é associado ao crescimento (ver p. 26), e o ponto de exclamação significa o fatorial, o número multiplicado por todos os outros números inteiros entre ele e 1 (ver p. 28). A letra grega lambda,

escrita como  $\lambda$ , é o número médio de mortes. Precisamos encontrar essa média em nossos 200 anos-batalhão, de modo que multiplicamos 0 mortes por 19 anos-batalhão (dando 0), 1 morte por 65 anos-batalhão (dando 65), 2 mortes por 22 anos-batalhão (dando 44), 3 mortes por 3 anos-batalhão (dando 9) e 4 mortes por 1 anos-batalhão (dando 4) e depois somamos todos (dando 122) e dividimos por 200. Então, nosso número médio de mortes por anos-batalhão é  $122/200=0,61$ .

$$e^{-\lambda} \lambda^x / x!$$

As probabilidades teóricas (que chamaremos de  $p$ ) podem ser encontradas substituindo os valores  $r = 0, 1, 2, 3$  e  $4$  na fórmula de Poisson. Os resultados são:

Número de mortes	0	1	2	3	4
Probabilidades, $p$	0,443	0,331	0,101	0,020	0,003
Número esperado de mortes, $200 \times p$	108,6	66,2	20,2	4,0	0,6

Parece que a distribuição teórica funcionou bem para os dados experimentais reunidos por Bortkiewicz.

**Primeiros números** Se analisarmos os últimos algarismos dos números numa coluna do catálogo de telefones, poderíamos esperar encontrar que 0, 1, 2,..., 9 estejam uniformemente distribuídos. Eles parecem aleatórios e qualquer número tem a mesma chance de aparecer. Em 1938, o engenheiro elétrico Frank Benford descobriu que isso não era verdade para os primeiros algarismos de alguns conjuntos de dados. De fato, ele redescobriu uma lei que tinha sido observada pela primeira vez pelo astrônomo Simon Newcomb em 1881.

Ontem, fiz uma pequena experiência. Dei uma olhada nas cotações de câmbio de moeda estrangeira num jornal. Havia taxas de câmbio como 2,119, dizendo que você precisava de US\$2,119 (dólares americanos) para comprar £1 (libra esterlina). Do mesmo modo, você vai precisar de €1,59 (euro) para comprar £1 esterlina e HK\$15,390 (dólares de Hong Kong) para comprar £1. Revendo os resultados dos dados e anotando o número de aparições do primeiro algarismo, obtive a seguinte tabela:

Primeiro dígito	1	2	3	4	5	6	7	8	9	total
Número de ocorrências	18	10	3	1	3	5	7	2	1	50
Porcentagem %	36	20	6	2	6	10	14	4	2	100

Esses resultados seguem a lei de Benford, que diz que, para algumas classes de dados, o número 1 aparece como primeiro algarismo em cerca de 30% dos casos, o número 2 em 18% e daí por diante. Certamente não se trata da distribuição uniforme que ocorre no último algarismo dos números de telefone.

Não é óbvio o motivo pelo qual tantos conjuntos de dados seguem a lei de Benford. No século XIX, quando Simon Newcomb observou isso no uso das tabelas matemáticas, ele mal podia adivinhar que esse uso dos conjuntos seria tão disseminado.

Exemplos em que a distribuição de Benford pode ser detectada incluem a marcação de pontos em eventos esportivos, dados do mercado de valores, números de casas, populações de países e o comprimento de rios. As unidades de medida não são importantes – não faz diferença se o comprimento dos rios é medido em metros ou milhas. A lei de Benford tem aplicações

práticas. Uma vez reconhecido que informações na contabilidade seguiam essa lei, tornou-se mais fácil detectar informações falsas e descobrir fraudes.

**Palavras** Um dos muitos interesses de G.K. Zipf era a prática pouco comum de contar palavras. Acontece que as dez mais populares palavras da língua inglesa são minúsculas, classificadas como mostrado:

Lugar	1	2	3	4	5	6	7	8	9	10
Palavra	<i>the</i>	<i>of</i>	<i>and</i>	<i>to</i>	<i>a</i>	<i>in</i>	<i>that</i>	<i>it</i>	<i>is</i>	<i>was</i>

Isso foi descoberto tomando-se uma grande amostra através de uma ampla gama de palavras escritas e simplesmente contando as palavras. A palavra mais comum recebeu a classificação 1, a segunda, classificação 2, e daí por diante. Pode haver pequenas diferenças no grau de popularidade, dependendo dos textos analisados, mas a variação não será grande.

Não é de surpreender que “*the*” (“o”) seja a mais comum e “*of*” (“do”) a segunda. A lista continua, e você pode achar interessante saber que “*amount*” (quantidade) está na 500ª posição e “*neck*” (pescoço) ficou em 100ª. Vamos considerar apenas as dez mais. Se você pegar um texto a esmo e contar essas palavras, vai obter mais ou menos as mesmas palavras na ordem de classificação. O fato surpreendente é que as classificações acompanham o real número de aparições das palavras no texto. A palavra “*the*” ocorrerá o dobro de vezes de “*of*”, com o triplo da frequência de “*and*”, e daí por diante. O número real é dado por uma fórmula bem conhecida. Essa é uma lei experimental e foi descoberta por Zipf a partir dos dados. A



lei teórica de Zipf diz que a porcentagem de ocorrências da palavra na classificação  $r$  é dada por

$$\frac{k}{r} \times 100$$

onde o número  $k$  depende apenas do tamanho do vocabulário do autor. Se um autor tem um alto domínio de todas as palavras na língua inglesa, das quais há cerca de um milhão, por algumas estimativas, o valor de  $k$  será em torno de 0,0694. Na fórmula para a lei de Zipf, a palavra “*the*” responderia então por cerca de 6,94% de todas as palavras em um texto. No mesmo modo “*of*” responderia por metade disso, ou cerca de 3,47% das palavras. Um ensaio com 3 mil palavras de um autor tão talentoso conteria, portanto, 208 ocorrências do “*the*” e 104 presenças da palavra “*of*”.

Para escritores com apenas 20 mil palavras à sua disposição, o valor de  $k$  se eleva a 0,0954, de modo que haveria 286 ocorrências do “*the*” e 143 aparecimentos de “*of*”. Quanto menor o vocabulário, mas frequentemente você vai ver aparecer o “*the*”.

**O olhar na bola de cristal** Seja Poisson, Benford ou Zipf, todas essas distribuições nos permitem fazer previsões. Pode ser que não possamos prever na mosca, mas saber como as probabilidades se distribuem é muito melhor do que dar um tiro no escuro. Além dessas três, acrescento outras distribuições, como a binominal, binominal negativa, geométrica, hipergeométrica e muitas mais, e o estatístico terá uma bela série de ferramentas para analisar uma vasta gama de atividades humanas.

**A ideia condensada:**

**prevendo quantos**

# 35 A curva normal

## linha do tempo

1733 d.C.	1820	1835	Década de 1870	1901
De Moivre publica obra sobre a curva normal como uma aproximação à distribuição binomial	Gauss usa a distribuição normal (chamada gaussiana) na astronomia como uma lei de erro	Quetelet usa a curva normal para medir a divergência em relação ao homem médio	A distribuição recebe o nome de "normal"	Aleksandr Lyapunov prova rigorosamente o teorema do limite central usando funções características

**A curva “normal” tem um papel fundamental na estatística. É considerada equivalente à linha reta na matemática. Certamente ela tem propriedades matemáticas importantes, mas se nos dedicarmos a analisar um bloco de dados em estado natural, raramente vamos observar que eles seguem exatamente uma curva normal.**

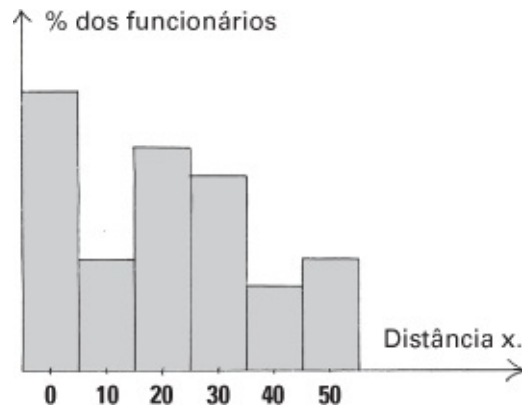
A curva normal é descrita por uma fórmula matemática específica que cria uma curva em forma de sino; uma curva com uma corcova terminando em uma cauda em cada uma das duas extremidades. A importância da curva normal está menos em sua natureza e mais na sua teoria, e nisso ela tem um longo pedigree. Em 1733, Abraham de Moivre, um huguenote francês que fugiu para a Inglaterra para escapar da perseguição religiosa, apresentou-a em conexão com sua análise das chances. Pierre Simon Laplace publicou resultados a respeito dela e Carl Friedrich Gauss a usou na astronomia, onde é algumas vezes chamada de lei gaussiana do erro.

Adolphe Quetelet usou a curva normal em seus estudos de sociologia publicados em 1835, onde mediu a divergência em relação ao “homem médio” pela curva normal. Em outras experiências, ele mediu a altura de recrutas franceses e a medida

do tórax de soldados escoceses e fez a suposição de que seguiam a curva normal. Naqueles dias havia uma forte crença de que, em sua maior parte, os fenômenos eram “normais”, nesse sentido.

**O coquetel** Vamos supor que Georgina tenha ido a um coquetel e o anfitrião, Sebastian, lhe perguntou se ela tinha vindo de longe. Ela se deu conta, mais tarde, de que era uma pergunta muito útil em coquetéis – aplica-se a qualquer pessoa e provoca uma resposta. Não é uma pergunta incômoda e quebra o gelo, se a conversa for difícil.

No dia seguinte, com uma leve ressaca, Georgina fez o trajeto para o escritório imaginando se seus colegas tinham vindo de longe para o trabalho. Na cantina dos funcionários, ficou sabendo que algumas pessoas moravam logo ali na esquina e que outros moravam a 80 quilômetros de distância – havia bastante variabilidade. Ela se aproveitou do fato de que era a gerente de Recursos Humanos de uma empresa muito grande para acrescentar a pergunta no final de seu questionário anual para os funcionários: “Que distância você viajou até o trabalho hoje?” Ela queria calcular a distância média do trajeto do pessoal da empresa. Quando Georgina traçou um histograma de resultados a distribuição não mostrou qualquer forma especial, mas pelo menos ela podia calcular a média da distância percorrida.

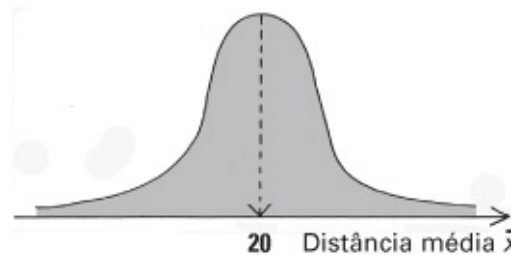


Histograma de Georgina da distância percorrida por seus colegas até o trabalho

Essa média acabou sendo de 32 quilômetros. Os matemáticos representam isso pela letra grega mu, escrita  $\mu$ , então aqui  $\mu = 32$ . A variação na população é representada pela letra grega sigma, escrita  $\sigma$ , que é algumas vezes chamada de desvio padrão. Se o desvio padrão for pequeno, os dados são próximos e têm variação pequena, mas se for grande, os dados estão espalhados. O analista de marketing da empresa, formado em estatística, mostrou a Georgiana que ela podia ter chegado ao mesmo valor de 32 por amostragem. Não havia necessidade de perguntar a *todos* os empregados. Essa técnica de estimativa depende do teorema do limite central.

Tome uma amostra aleatória dos funcionários da força de trabalho inteira da empresa. Quando maior a amostra, melhor, mas 30 funcionários já funcionam bem. Ao selecionar essa amostra a esmo, é provável que haja funcionários que morem logo ali na esquina e também alguns que viajem de longe. Quando calculamos a distância média para nossa amostra, o efeito das distâncias maiores será puxado para a média pelo das distâncias mais curtas.

Os matemáticos escrevem a média de uma amostra como  $\bar{x}$ , lido como “ $\bar{x}$  barra”. No caso da Georgina, é mais provável que o valor de  $\bar{x}$  seja próximo a 32, a média da população. Embora isso seja certamente possível, é pouco provável que a média da amostra seja muito pequena ou muito grande.



Como a média da amostra é distribuída.

O teorema do limite central é um dos motivos pelos quais a curva normal é importante para os estatísticos. Ele declara que a distribuição real das médias das amostras  $\bar{x}$  se aproxima de uma curva normal, não importando a distribuição de  $\chi$ . O que isso significa? No caso de Georgina,  $\chi$  representa a distância do local de trabalho e  $\bar{x}$  é a média de uma amostra.

A distribuição de  $\chi$  no histograma de Georgina não se parece nem um pouco com uma curva em sino, mas a distribuição de  $\bar{x}$  é e está centrada em  $\mu = 32$ .

É por isso que podemos usar a média de uma amostra  $\bar{x}$  como uma estimativa da média da população,  $\mu$ . A variação das médias das amostras,  $\bar{x}$ , é um bônus a mais. Se a variação dos valores de  $\chi$  é o desvio padrão  $\sigma$ , a variação de  $\bar{x}$  é  $\sigma/\sqrt{n}$ , onde  $n$  é tamanho da amostra escolhida. Quanto maior o tamanho da amostra, mais estreita será a curva normal, e melhor será a estimativa de  $\mu$ .

**Outras curvas normais** Façamos um experimento simples. Vamos jogar uma moeda quatro vezes. A chance de jogar uma cara a cada vez é de  $p = 1/2$ . O resultado de quatro jogadas pode ser anotado usando  $H$  para cara e  $T$  para coroa, arrumados na ordem em que ocorrerem. No total há 16 resultados possíveis. Por exemplo, podemos obter três caras no resultado  $THHH$ . Na verdade, há quatro resultados possíveis, dando três caras (os demais são  $HTHH$ ,  $HHTH$ ,  $HHHT$ ), de modo que a probabilidade de três caras é de  $4/16 = 0,25$ .

Com um número pequeno de jogadas, as probabilidades são calculadas facilmente e dispostas em uma tabela, e podemos também calcular como as probabilidades estão distribuídas. A linha do número de combinações pode ser encontrada a partir do triângulo de Pascal (ver p. 52):

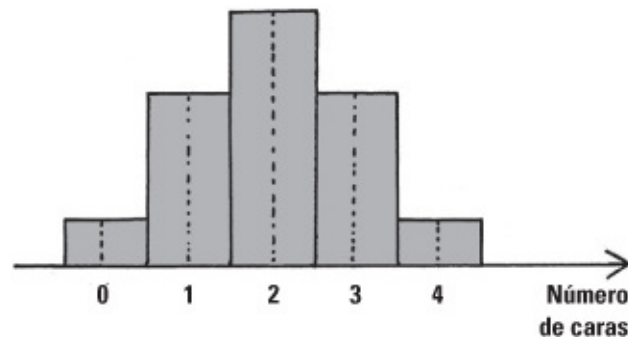
Número de caras	0	1	2	3	4
Número de combinações	1	4	6	4	1
Probabilidade	0,0624	0,25	0,376	0,25	0,0625
	(= 1/16)	(= 4/16)	(= 6/16)	(= 4/16)	(= 1/16)

Isso é chamado de distribuição binomial de probabilidades, que ocorre quando há dois resultados possíveis (aqui, uma cara ou uma coroa). Essas probabilidades podem ser representadas por um diagrama, no qual são descritas tanto pela altura quanto pelas áreas.

Jogar uma moeda quatro vezes é um tanto restritivo. O que acontece se jogarmos mais vezes, digamos 100? Pode-se aplicar a distribuição binomial das probabilidades, onde  $n=100$ , mas essa distribuição pode ser proveitosamente aproximada pela

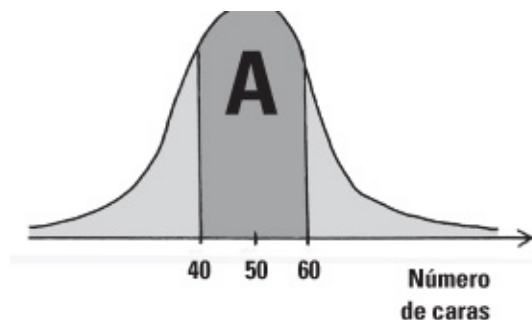


curva de sino normal com média  $\mu = 50$  (já que esperaríamos 50 caras ao jogar uma moeda 50 vezes) e a variação (desvio padrão) de  $\sigma = 5$ . Foi isso que de Moivre descobriu no século XVI.



O número de caras em quatro jogadas de uma moeda, de acordo com a distribuição binomial

Para valores grandes de  $n$ , a variável  $x$  que mede o número de sucessos se ajusta cada vez melhor à curva normal. Quanto maior o valor de  $n$ , melhor a aproximação, e jogar a moeda 100 vezes é bem grande. Agora, digamos que queremos saber a probabilidade de jogar entre 40 e 60 caras, que escrevemos como  $prob(40 \leq x \leq 60)$ . Para encontrar o verdadeiro valor numérico, precisamos usar tabelas matemáticas pré-calculadas, e uma vez feito isso, encontramos  $prob(40 \leq x \leq 60) = 0,9545$ . Isso mostra que temos 95,45% de probabilidade de obter entre 40 e 60 caras ao jogarmos 100 vezes, o que significa que é muito provável.



Distribuição da probabilidade do número de caras em 100 jogadas de uma

moeda

A área que sobra é  $1 - 0,9545$ , que são meros  $0,0455$ . Como a curva normal é simétrica em relação ao meio, metade disso dará a probabilidade de se obter mais de 60 caras em 100 jogadas da moeda. Isso é apenas  $2,275\%$  e representa uma chance muito pequena mesmo. Se você visitar Las Vegas, essa seria uma aposta a ser deixada de lado.

**A ideia condensada:  
a onipresente curva  
em forma de sino**

## 36 Conectando dados

### linha do tempo

1806 d.C.	1809	1885-8	1896	1953
Adrien-Marie Legendre ajusta dados por mínimos quadrados	Carl Friedrich Gauss usa o método dos mínimos quadrados em problemas astronômicos	Galton introduz a regressão e a correlação	Pearson publica contribuições à correlação e regressão	Spearman usa correlação de classificação como ferramenta de estudos psicológicos

**Como são conectados dois conjuntos de dados? Os estatísticos de cem anos atrás achavam que tinham a resposta. Correlação e regressão andam juntas como corda e caçamba, mas como esses emparelhamentos, elas são diferentes e têm suas próprias tarefas a cumprir. A correlação mede como quantidades como peso e altura estão relacionadas uma à outra. A regressão pode ser usada para prever os valores de uma propriedade (digamos, peso) a partir da outra (nesse caso, altura).**

**Correlação de Pearson** O termo correlação foi introduzido por Francis Galton nos anos 1880. Ele originalmente o chamou de “correlação”, uma palavra melhor para explicar seu significado. Galton, um cavalheiro vitoriano afeito à ciência, tinha o desejo de medir tudo, e aplicava a correlação às suas investigações de pares de variáveis: o comprimento da asa e da cauda de aves, por exemplo. O coeficiente de correlação de Pearson, que recebeu o nome em homenagem a Karl Pearson, biógrafo e pupilo de Galton, é medido em uma escala entre menos um e mais um. Se seu valor numérico for, digamos, + 0,9, diz-se que há uma forte correlação entre as variáveis. O coeficiente de correlação mede a tendência dos dados a se posicionarem sobre uma linha reta. Se for próximo a zero, a correlação é praticamente inexistente.

Muitas vezes queremos desenvolver uma correlação entre duas variáveis para ver o quão fortemente elas estão conectadas. Vamos pegar o exemplo das vendas de óculos de sol e ver como isso está relacionado à venda de sorvetes. San Francisco seria um bom lugar para realizar esse estudo, e vamos reunir dados a cada mês nessa cidade. Se marcarmos os pontos em um gráfico em que a coordenada  $x$  (horizontal) representa a venda de óculos e a coordenada  $y$  (vertical) dá a venda de sorvetes, todos os meses teremos um ponto de dados  $(x, y)$ , representando os dois tipos de dados. Por exemplo, o ponto  $(3, 4)$  pode significar que a venda de óculos em maio foi de US\$30 mil, enquanto a venda de sorvetes na cidade foi de US\$40 mil no mesmo mês. Podemos lançar em gráfico os pontos de dados  $(x, y)$  para um ano inteiro em um diagrama de dispersão. Para esse exemplo, o valor da correlação de Pearson seria em torno de  $+0,9$ , indicando uma forte correlação. Os dados têm uma tendência a seguir uma linha reta. É positiva porque a linha tem um gradiente positivo – está apontando para a direção nordeste.

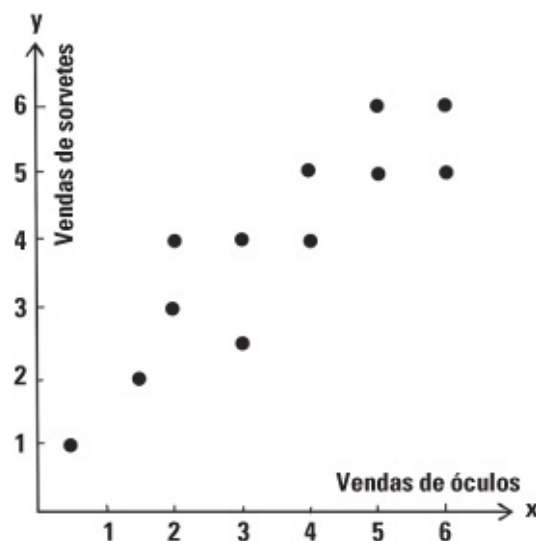


Diagrama de dispersão

**Causa e correlação** Encontrar uma correlação forte entre duas variáveis não basta para alegar que uma causa a outra. Pode haver uma relação de causa e efeito entre as duas variáveis, mas isso não pode ser alegado apenas com base na evidência numérica. Na questão da causa/correlação, costuma-se usar a palavra “associação” e é sensato desconfiar antes de afirmar mais do que isso.

No exemplo dos óculos de sol e dos sorvetes, há uma forte correlação entre as vendas dos óculos e dos sorvetes. Quando a venda dos óculos aumenta, o consumo de sorvetes tende a aumentar. Seria absurdo alegar que o gasto em óculos de sol provocou uma maior venda de sorvetes. Nas correlações pode haver alguma variável intermediária trabalhando ocultamente. Por exemplo, as despesas com óculos de sol e sorvetes se conectam com o resultado de efeitos sazonais (tempo quente nos meses de verão, tempo frio no inverno). Há um outro perigo ao usar correlação. Pode haver uma correlação forte entre o número da casa e as idades combinadas dos ocupantes das casas, mas ler qualquer significado nisso seria um desastre.

**Correlação de Spearman** A correlação pode ser posta a outros usos. O coeficiente de correlação pode ser adaptado para tratar dados ordenados – dados nos quais queremos saber o primeiro, segundo, terceiro, e daí por diante, mas não necessariamente outros valores numéricos.

Ocasionalmente só temos as classificações, como dados. Vejamos Albert e Zac, dois severos juízes de patinação no gelo numa competição em que têm de avaliar os patinadores no mérito

artístico. Será uma avaliação subjetiva. Tanto Albert como Zac são medalhistas olímpicos e são chamados para julgar o último grupo, que foi reduzido a cinco competidores: Ann, Beth, Charlotte, Dorothy e Ellie. Se Albert e Zac os classificarem exatamente do mesmo modo, ótimo, mas a vida não é assim. Por outro lado, não podemos esperar que Albert as qualifique de um jeito e Zac as classifique exatamente na ordem inversa. A realidade é que as qualificações deverão estar entre esses dois extremos. Alberto as classificou de 1 a 5 com Ann (a melhor) seguida por Ellie, Beth, Charlotte e finalmente Dorothy na 5ª posição. Zac classificou Ellie como a melhor, seguida de Beth, Ann, Dorothy e Charlotte.

Essa classificação pode ser resumida em uma tabela:

Patinadora	Classificação de Albert	Classificação de Zac	Diferença nas classificações, d	d <sup>2</sup>
Ann	1	3	-2	4
Ellie	2	1	1	1
Beth	3	2	1	1
Charlotte	4	5	-1	1
Dorothy	5	4	1	1
n=5			Soma	8

Como podemos medir o nível de concordância entre os juízes? O coeficiente de correlação de Spearman é o instrumento que os matemáticos usam para fazer essa medida para dados ordenados. Seu valor aqui é +0,6, que indica uma medida limitada de concordância entre Albert e Zac. Se tratarmos os pares de classificações como pontos, podemos lançá-los em um gráfico para obter uma representação visual da proximidade na

opinião dos dois juízes.

$$1 - \frac{6 \times \text{Sum}}{n \times (n^2 - 1)}$$

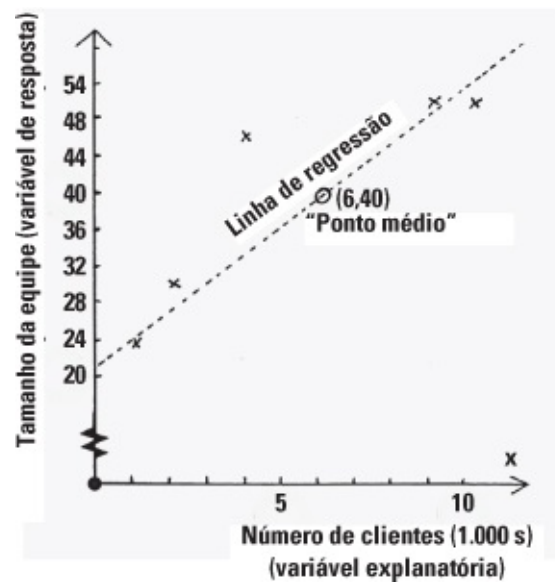
Fórmula de Spearman

A fórmula para esse coeficiente de correlação foi desenvolvida em 1904 por Charles Spearman, que como Pearson, foi influenciado por Francis Galton.

**Linhas de regressão** Você é mais baixa ou mais alta do que seus dois genitores ou está entre as alturas deles? Se fôssemos todos mais altos do que nossos pais, e isso acontecesse em cada geração, então um dia a população poderia ser composta de pessoas de 3 metros ou mais, e certamente isso é impossível. Se fôssemos todos mais baixos do que nossos pais, então a população iria aos poucos diminuir em altura, e isso é igualmente improvável. A verdade está em algum outro lugar.

Francis Galton desenvolveu experiências nos anos 1880, comparando a altura de jovens adultos maduros com a altura de seus pais. Para cada valor da variável  $x$ , que media a altura dos pais (na verdade combinando a altura da mãe com a do pai na medida “genitor médio”), ele observou as alturas de sua prole. Estamos falando aqui a respeito de um cientista prático, de modo que lá vieram os lápis e folhas de papel divididas em quadrados nas quais ele lançou os dados. Para 205 genitores médios e 928 rebentos ele encontrou que a altura média dos dois conjuntos era de 173,4 cm, valor que ele chamou de mediocridade. Ele verificou que os filhos de genitores médios

muito altos eram em geral mais altos do que essa mediocridade, mas não tão altos quanto seus genitores médios, enquanto crianças mais baixas eram mais altas do que seus genitores médios, mas mais baixos do que a mediocridade. Em outras palavras, a altura das crianças regredia na direção da mediocridade.



A regressão é uma técnica poderosa e amplamente aplicável. Suponhamos que, para um levantamento, o time de pesquisa operacional de uma cadeia de varejo popular escolha 5 de suas lojas, de pequenos pontos de venda (com 1.000 fregueses por mês), até *megastores* (com 10 mil fregueses por mês). A equipe de pesquisa observa o número do quadro de funcionários em cada uma. Eles planejam usar a regressão para estimar quantos empregados vão precisar para suas outras lojas.

Número de fregueses (em 1.000)	1	4	6	9	10
Número de empregados	24	30	46	47	53

Vamos lançar isso num gráfico, em que chamaremos a



coordenada  $x$  de número de fregueses (chamamos isso de variável explanatória), enquanto o número de empregados é lançado como a coordenada  $y$  (chamada de variável de resposta). É o número de fregueses que explica o número de empregados necessários, não o contrário. O número médio de fregueses nas lojas é lançado como 6 (ou seja, 6 mil fregueses) e o número médio de empregados nas lojas é 40. A linha de regressão sempre passa pelo “ponto médio”, aqui (6,40). Há fórmulas para calcular a linha de regressão, a linha que melhor ajusta os dados (também chamada de linha dos “mínimos quadrados”). No nosso caso a linha é  $y = 20,8 + 3,2x$ , de modo que a inclinação é 3,2 e positiva (sobe da esquerda para a direita). A linha cruza o eixo vertical dos  $y$  no ponto 20,8. O termo  $y$  é a estimativa do valor de  $y$  obtido a partir da linha. Então, se quisermos saber quantos empregados devem ser contratados em uma loja que recebe 5 mil fregueses por mês podemos substituir o valor  $x = 5$  na equação de regressão e obter a estimativa  $y$  empregados, mostrando como a regressão tem um objetivo muito prático.

## A ideia condensada: a interação dos dados

# 37 Genética

## linha do tempo

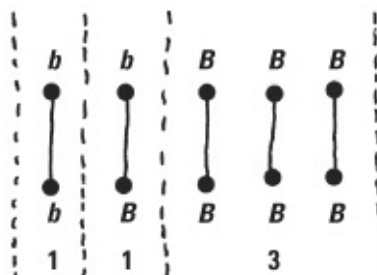
1718 d.C.	1865	1908	1918	1953
Abraham de Moivre publica <i>Doctrine of Chances</i>	Mendel propõe a existência de genes e as leis da hereditariedade	Hardy e Weinberg mostram porque genes dominantes não suplantam genes recessivos	Fisher reconcilia a teoria de Darwin com a teoria da hereditariedade de Mendel	É descoberta a estrutura em dupla-hélice do DNA

A genética é um ramo da biologia, então por que estaria em um livro de matemática? A resposta é que esses dois assuntos fazem uma fertilização cruzada e se enriquecem mutuamente. Os problemas da genética exigem matemática, mas a genética também sugeriu novos ramos de álgebra. Gregor Mendel é fundamental para todo o tema da genética, o estudo da herança humana. Características hereditárias, como cor dos olhos, cor do cabelo, daltonismo, domínio da mão direita ou da esquerda e grupo sanguíneo são determinadas por fatores (alelos) de um gene. Mendel disse que esses fatores passam para a geração seguinte de forma independente.

Então, como é que o fator cor do olho pode ser transmitido para a geração seguinte? No modelo básico há dois fatores,  $b$  e  $B$ :

$b$  é o fator para olhos azuis

$B$  é o fator para olhos castanhos



População representando as proporções 1:1:3 dos genótipos  $bb$ ,  $bB$  e  $BB$ .

Nos indivíduos, os fatores aparecem em pares, dando surgimento a possíveis genótipos  $bb$ ,  $bB$  e  $BB$  (porque  $bB$  é o mesmo que  $Bb$ ). Uma pessoa carrega um desses três genótipos, que determinam a cor do olho. Por exemplo, uma população pode consistir em um quinto das pessoas com o genótipo  $bb$ , outro quinto com o genótipo  $bB$  e os restantes três quintos com o genótipo  $BB$ . Em termos de porcentagens, esses genótipos podem perfazer 20%, 20% e 60% da população. Isso pode ser representado por um diagrama que mostra essas proporções de genótipos.

O fator  $B$ , que denota a cor de olho castanho, é o fator dominante e  $b$ , a cor do olho azul, é o fator recessivo. Uma pessoa com genes puros do genótipo  $BB$  terá olhos castanhos, mas também os terá uma pessoa com fatores mistos, ou seja, os que tenham um genótipo híbrido  $bB$ , porque o  $B$  é dominante. Uma pessoa com genes puros de genótipo  $bb$  será o único genótipo a exibir olhos azuis.

Uma questão instigante no campo da biologia surgiu no início do século XIX. Será que os olhos castanhos iriam eventualmente dominar e os olhos azuis sumiriam? Será que os olhos azuis se tornariam extintos? A resposta foi um sonoro “não”.

**A lei de Hardy-Weinberg** Isso foi explicado pela lei de Hardy-Weinberg, uma aplicação da matemática básica à genética. Ela explica como, na teoria mendeliana da hereditariedade, um gene dominante não assume completamente e um gene recessivo não desaparece.

G.H. Hardy era um matemático inglês que se orgulhava da não aplicabilidade da matemática. Ele era um grande pesquisador da matemática pura, mas é provavelmente mais conhecido por sua única contribuição à genética – que surgiu como um cálculo improvisado às pressas, depois de uma partida de críquete. Wilhelm Weinberg veio de um meio muito diferente. Clínico geral na Alemanha, foi geneticista a vida toda. Ele descobriu a lei ao mesmo tempo que Hardy, por volta de 1908.

A lei está relacionada a uma grande população, na qual os casamentos ocorrem ao acaso. Não há emparelhamentos preferenciais, de modo que, por exemplo, pessoas de olhos azuis não preferem se casar com pessoas de olhos azuis. Quando procriam, a criança recebe um fator de cada genitor. Por exemplo, um genótipo híbrido  $bB$  ao se casar com um híbrido  $bB$  pode produzir qualquer um de  $bb$ ,  $bB$ ,  $BB$ , mas um casamento de  $bb$  com  $BB$  só pode produzir um híbrido,  $bB$ . Qual é a probabilidade de ser transmitido um fator  $b$ ? Contando o número de fatores  $b$ , há dois fatores  $b$  para cada genótipo  $bb$  e um fator  $b$  para cada genótipo  $bB$ , dando, como proporção, um total de três fatores  $b$  em 10 (no nosso exemplo de uma população com proporções 1:1:3 para os três genótipos). A probabilidade de transmissão de um fator  $b$  ser incluído no genótipo de uma criança é, portanto,  $3/10$  ou  $0,3$ . A probabilidade de transmissão da inclusão de um fator  $B$  é  $7/10$ , ou  $0,7$ . A probabilidade do genótipo  $bb$  ser incluído na geração seguinte, por exemplo, é, portanto,  $0,3 \times 0,3 = 0,9$ . O conjunto completo das probabilidades está resumido na tabela:

fator	<i>b</i>		<i>B</i>	
<i>b</i>	<i>bb</i>	$0,3 \times 0,3 = 0,09$	<i>bB</i>	$0,3 \times 0,7 = 0,21$
<i>B</i>	<i>Bb</i>	$0,3 \times 0,7 = 0,21$	<i>BB</i>	$0,7 \times 0,7 = 0,49$

Os genótipos híbridos *bB* e *Bb* são idênticos, então a probabilidade de eles ocorrerem é  $0,21 + 0,21 = 0,42$ . Expressos como porcentagem, as taxas de genótipos *bb*, *bB* e *BB* na nova geração são 9%, 42% e 49%. Como o *B* é o fator dominante,  $42\% + 49\% = 91\%$  da primeira geração terão olhos castanhos. Apenas um indivíduo com genótipo *bb* vai apresentar as características observáveis do fator *b*, então apenas 9% da população terá olhos azuis.

A distribuição inicial dos genótipos era 20%, 20% e 60%, e na nova geração a distribuição dos genótipos é 9%, 42% e 49%. O que acontece em seguida? Vamos ver o que acontece se uma nova geração é obtida a partir dessa por casamento aleatório. A proporção de fatores *b* é  $0,09 + 1/2 \times 0,42 = 0,3$ , a proporção de fatores *B* é  $1/2 \times 0,42 + 0,49 = 0,7$ . Essas são idênticas às probabilidades de transmissão anteriores dos fatores *b* e *B*. A distribuição dos genótipos *bb*, *bB* e *BB* na geração seguinte é, portanto, a mesma que a da geração anterior, e em particular o genótipo *bb*, que dá olhos azuis, não desaparece, mas permanece estável em 9% da população. Proporções sucessivas de genótipos durante uma sequência de casamentos aleatórios são, portanto,

$$20\%, 20\%, 60\% \rightarrow 9\%, 42\%, 49\% \rightarrow \dots \rightarrow 9\%, 42\%, 49\%$$

Isso está de acordo com a lei de Hardy-Weinberg: depois da primeira geração, as proporções do genótipo permanecem constantes de geração a geração, e as probabilidades de

transmissão também são constantes.

**Argumento de Hardy** Para ver se a lei de Hardy-Weinberg funciona para qualquer população inicial, não apenas para a de 20%, 20% e 60% que escolhemos para o nosso exemplo, não há melhor maneira do que buscar o argumento do próprio Hardy, que ele escreveu ao editor do periódico norte-americano *Science* em 1908.

Hardy começa com a distribuição inicial de genótipos  $bb$ ,  $bB$  e  $BB$  como  $p$ ,  $2r$  e  $q$  e as probabilidades de transmissão  $p + r$  e  $r + q$ . No nosso exemplo numérico (de 20%, 20% e 60%),  $p = 0,2$ ,  $2r = 0,2$  e  $q = 0,6$ . As probabilidades de transmissão dos fatores  $b$  e  $B$  são  $p + r = 0,2 + 0,1 = 0,3$  e  $r + q = 0,1 + 0,6 = 0,7$ . E se houvesse uma distribuição inicial diferente dos genótipos  $bb$ ,  $bB$  e  $BB$  e começássemos com, digamos, 10%, 60% e 30%? Como é que a lei de Hardy-Weinberg funcionaria nesse caso? Aqui teríamos  $p = 0,1$ ,  $2r = 0,6$  e  $q = 0,3$ , e nas probabilidades de transmissão os fatores  $b$  e  $B$  são, respectivamente,  $p + r = 0,4$  e  $r + q = 0,6$ . Então, a distribuição da geração seguinte de genótipos é 16%, 48% e 36%. Proporções sucessivas dos genótipos  $bb$ ,  $bB$  e  $BB$  depois de casamentos aleatórios são

$$10\%, 60\%, 30\% \rightarrow 16\%, 48\%, 36\% \rightarrow \dots \rightarrow 16\%, 48\%, 36\%$$

A proporção se estabiliza depois de uma geração, como antes, e a probabilidade das transmissões de 0,4 e 0,6 permanece constante. Com esses números 16% da população terá olhos azuis e 48% + 84% terão olhos castanhos porque  $B$  é dominante no genótipo  $bB$ .

Então, a lei de Hardy-Weinberg implica que essas proporções de genótipos,  $bb$ ,  $bB$  e  $BB$  permanecerão constantes de geração a geração, não importa qual a distribuição dos fatores na população. O gene dominante  $B$  não prevalece e as proporções dos genótipos são intrinsecamente estáveis.

Hardy acentuou que esse modelo era apenas aproximado. Sua simplicidade e elegância dependiam de muitas suposições que não se sustentam na vida real. No modelo, a probabilidade de mutação de genes ou de mudanças nos genes propriamente ditos foi descontada, e a consequência de as proporções de transmissão serem constantes significa que esse modelo não tem nada a dizer a respeito da evolução. Na vida real há a “inclinação genética” e as probabilidades de transmissão dos fatores não permanecem constantes. Isso provocará variações nas proporções totais e novas espécies vão evoluir.

A lei de Hardy-Weinberg aproximou a teoria de Mendel – a “teoria quântica” da genética –, o darwinismo e a seleção natural em um modo intrínseco. Foi preciso esperar o gênio de R.A. Fisher para reconciliar a teoria mendeliana da hereditariedade com a teoria contínua em que as características evoluem.

O que estava faltando na ciência da genética até os anos 1950 era uma compreensão física do material genético propriamente dito. Então, houve um avanço significativo, que foi a contribuição de Francis Crick, James Watson, Maurice Wilkins e Rosalind Franklin. O meio era o ácido desoxirribonucleico, ou DNA. É preciso matemática para modelar a famosa dupla-hélice (ou um

par de espirais enroladas em torno de um cilindro). Os genes estão localizados em segmentos dessa dupla-hélice.

A matemática é indispensável no estudo da genética. Desde a geometria básica das espirais do DNA e a potencialmente sofisticada lei de Hardy-Weinberg, têm sido desenvolvidos modelos matemáticos lidando com muitas características (não apenas cor dos olhos), incluindo diferenças entre homens e mulheres e também casamentos não aleatórios. A ciência da genética tem também retribuído o cumprimento à matemática, sugerindo novos ramos de álgebra abstrata de interesse por suas intrigantes propriedades matemáticas.

**A ideia condensada:  
incerteza no pool  
genético**



# 38 Grupos

## linha do tempo

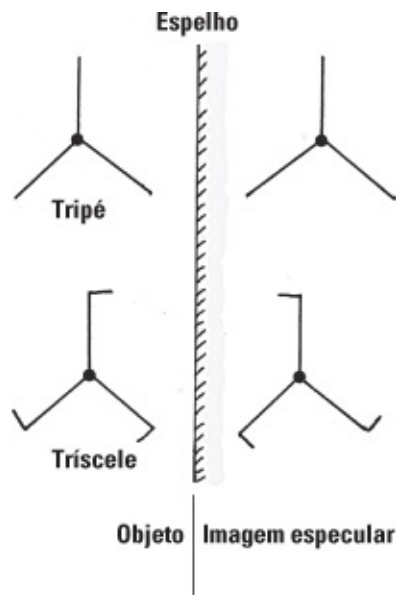
1832 d.C.	1854	1872	1891	1983
Galois propõe a ideia de grupos de permutações	Cayley tenta generalizar o conceito de grupo	Felix Klein começa um programa para classificar a geometria usando grupos	Evgraf Fedorov e Arthur Schönflies classificam independentemente os 230 grupos cristalográficos	A classificação de grupos simples finitos é completada e o teorema enorme é provado

**Evariste Galois morreu num duelo aos 20 de idade, mas deixou ideias em número suficiente para manter matemáticos ocupados durante séculos. Essas ideias envolviam a teoria dos grupos, construtos matemáticos que podem ser usados para quantificar simetria. Fora o apelo artístico, a simetria é o ingrediente essencial para cientistas que sonham com uma futura teoria de tudo. A teoria dos grupos é a cola que une o “tudo”.**

Estamos rodeados por simetria. Os vasos gregos a têm, os flocos de neve a têm, construções frequentemente a têm e algumas letras do nosso alfabeto também a têm. Há diversos tipos de simetria: as principais são a simetria especular e a simetria rotacional. Vamos examinar apenas simetrias bidimensionais – todos os nossos objetos de estudo moram na superfície plana desta página.

**Simetria especular** Será que podemos instalar um espelho de modo tal que os objetos apareçam de forma igual à frente do espelho e no espelho? A palavra MUM tem simetria especular, mas HAM, não; MUM em frente ao espelho é o mesmo que MUM no espelho, enquanto HAM se torna MAH. Um tripé tem simetria especular, mas o tríscele (um tripé com três pés) não tem. O tríscele, como o objeto à frente do espelho, é destro, mas a

imagem no espelho no que é chamado de plano da imagem é canhoto.



**Simetria rotacional** Podemos também indagar se há um eixo perpendicular à página, de modo que o objeto possa ser rodado em um ângulo na página e ser trazido de volta à sua posição original. Tanto o tripé quanto o tríscele têm simetria rotacional. O tríscele, que significa “três pernas”, é uma forma interessante. A versão destra é uma figura que aparece como o símbolo da Ilha de Man e também na bandeira da Sicília.



O tríscele da Ilha de Man

Se fizermos uma rotação de  $120^\circ$  ou  $240^\circ$ , a figura rodada vai coincidir com ela mesma; se você fechar os olhos antes de rodá-la, verá o mesmo tríscele quando os abrir outra vez depois da rotação.

O curioso sobre a figura de três pernas é que, se mantida no plano, não importa o número de rotações, jamais converterá um tríscele orientado para a direita em um outro orientado para a esquerda. Objetos cuja imagem no espelho é diferente do objeto em frente ao espelho são chamados de quirais – elas parecem semelhantes, mas não são as mesmas. A estrutura molecular de alguns compostos químicos pode existir tanto na forma dextrogira quanto na forma levogira nas três dimensões e são exemplos de objetos quirais. Esse é o caso do composto limoneno, que em uma forma tem gosto de limão e na outra, de laranja. A droga talidomida sob uma forma é um eficaz remédio contra enjoo matinal na gravidez, mas sob a outra forma tem consequências trágicas.

**Medida da simetria** No caso do nosso tríscele, as operações básicas de simetria são (sentido horário) rotações  $R$  de  $120^\circ$  e  $S$  de  $240^\circ$ . A transformação  $I$  é a que roda o triângulo em  $360^\circ$  ou, alternativamente, não faz nada. Podemos criar uma tabela baseada nas combinações dessas rotações, do mesmo modo que podemos criar uma tabela de multiplicação.

Essa tabela parece uma tabela de multiplicação comum com números, só que estamos “multiplicando” símbolos. De acordo com a convenção amplamente usada, a multiplicação  $R \circ S$  significa rodar o tríscele no sentido horário em  $240^\circ$  com  $S$  e

depois em  $120^\circ$  com  $R$ , o resultado sendo uma rotação de  $360^\circ$ , como se você não tivesse feito nada. Isso pode ser expresso como  $R \circ S = I$ , o resultado encontrado na junção da penúltima fileira com a última coluna da tabela.

$\circ$	$I$	$R$	$S$
$I$	$I$	$R$	$S$
$R$	$R$	$S$	$I$
$S$	$S$	$I$	$R$

Tabela de Cayley para o grupo de simetria do tríscele

O grupo de simetria do tríscele é feito sobre  $I$ ,  $R$  e  $S$  e a tabela de multiplicação de como os combinar. Como o grupo contém três elementos, seu tamanho (ou “ordem”) é três. A tabela é também chamada de tabela de Cayley (em homenagem ao matemático Arthur Cayley, primo distante de sir George Cayley, um pioneiro da aviação).

Da mesma maneira que o tríscele, o tripé sem pés tem simetria rotacional. Mas tem também simetria especular e, portanto, tem um grupo de simetria maior. Vamos chamar de  $U$ ,  $V$  e  $W$  as reflexões nos três eixos do espelho.

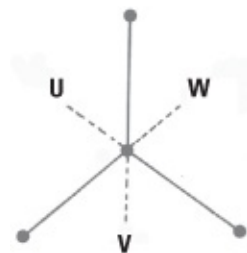
$\circ$	$I$	$R$	$S$	$U$	$V$	$W$
$I$	$I$	$R$	$S$	$U$	$V$	$W$
$R$	$R$	$S$	$I$	$V$	$W$	$U$
$S$	$S$	$I$	$R$	$W$	$U$	$V$
$U$	$U$	$W$	$V$	$I$	$S$	$R$
$V$	$V$	$U$	$W$	$R$	$I$	$S$
$W$	$W$	$V$	$U$	$S$	$R$	$I$

Tabela de Cayley para o grupo de simetria do tripé

O grupo de simetria maior do tripé é de ordem seis, é composto de seis transformações,  $I$ ,  $R$ ,  $S$ ,  $U$ ,  $V$  e  $W$ , e a tabela de multiplicação está mostrada.

É alcançada uma transformação interessante pela combinação de dois reflexos em eixos diferentes, como  $U \circ W$  (onde o reflexo de  $W$  é aplicado primeiro e é seguido pelo reflexo  $U$ ). Isso é na verdade uma rotação do tripé de  $120^\circ$ , em símbolos  $U \circ W = R$ . Combinando os reflexos ao contrário,  $W \circ U = S$  dá uma rotação de  $240^\circ$ . Em particular  $U \circ W \neq W \circ U$ . Isso é uma grande diferença entre uma tabela de multiplicação para um grupo e uma tabela de multiplicação comum com números.

Um grupo em que a ordem de combinação dos elementos é imaterial é chamado de grupo abeliano, em homenagem ao matemático norueguês Niels Abel. O grupo de simetria do tripé é o menor grupo que não é abeliano.



Reflexos de um tripé

**Grupos abstratos** A tendência na álgebra do século XX tem sido na direção da álgebra abstrata, na qual um grupo é definido por algumas regras básicas conhecidas com axiomas. Com esse ponto de vista, o grupo de simetria do triângulo se torna apenas mais um exemplo de um sistema abstrato. Há sistemas na álgebra que são mais básicos do que um grupo e exigem menos

axiomas; outros sistemas que são mais complexos exigem mais axiomas. Entretanto, o conceito de grupo está exatamente certo e é o sistema algébrico mais importante de todos. É notável que de tão poucos axiomas tenha surgido um corpo de conhecimentos tão grande. A vantagem do método abstrato é que em geral os teoremas podem ser deduzidos para todos os grupos e aplicados, se for preciso, a grupos específicos.

Uma característica da teoria do grupo é que pode haver grupos menores dentro dos maiores. O grupo de simetria do tríscele de ordem três é um subgrupo do grupo de simetria do tripé, de ordem seis. J.L. Lagrange provou um fato básico a respeito dos subgrupos. O teorema de Lagrange determina que a ordem de um subgrupo deve sempre dividir exatamente a ordem do grupo. Então nós automaticamente sabemos que o grupo de simetria do tripé não tem subgrupo de ordem quatro ou cinco.

**Classificação de grupos** Tem havido um vasto programa para classificar todos os grupos finitos possíveis. Não há necessidade de enumerá-los porque alguns grupos são construídos e outros são básicos, e são os básicos que são necessários. O princípio da classificação é muito semelhante à classificação na química, onde o interesse está focalizado nos elementos químicos básicos e não nos compostos que podem ser feitos com eles. O grupo de simetria do tripé de seis elementos é um “composto” construído de um grupo de rotações (de ordem três) e de reflexos (de ordem dois).

## Axiomas para um grupo

Uma coleção de elementos  $G$  com “multiplicação”  $\circ$  é chamada de grupo se

1. Existe um elemento  $1$  em  $G$ , de modo que  $1^\circ = a = a^\circ 1 = a$  para todos os elementos  $a$  no grupo  $G$  (o elemento especial  $1$  é chamado de elemento de identidade).
2. Para cada elemento  $a$  em  $G$ , há um elemento  $\tilde{a}$  em  $G$  com  $\tilde{a}^\circ a = a^\circ \tilde{a} = 1$  (o elemento  $\tilde{a}$  é chamado de inverso do elemento  $a$ ).
3. Para todos os elementos  $a, b$  e  $c$  em  $G$ , é verdadeiro que  $a^\circ (b^\circ c) = (a^\circ b)^\circ c$  (isso é chamado de lei associativa).

Praticamente todos os grupos básicos podem ser classificados em classes conhecidas. A classificação completa, chamada de “o teorema enorme”, foi anunciada por Daniel Gorenstein em 1983 e alcançada através do trabalho acumulado de 30 anos de pesquisa e publicações por matemáticos. É o atlas de todos os grupos conhecidos. Os grupos básicos caem dentro de um de quatro tipos principais, no entanto, foram encontrados 26 grupos que não caem em nenhuma categoria. Esses são conhecidos como os grupos esporádicos.

Os grupos esporádicos são dissidentes e em geral têm ordem mais alta. Cinco dos menores eram conhecidos por Émile Mathieu nos anos 1860, mas grande parte da atividade moderna aconteceu entre 1965 e 1975. O menor grupo esporádico é de ordem  $7.920 = 2^4 \times 3^2 \times 5 \times 11$ , mas na extremidade superior

estão o “bebê monstro” e o “monstro” simples, que tem ordem  $2^{46} \times 3^{20} \times 5^9 \times 7^6 \times 11^2 \times 13^3 \times 17 \times 19 \times 23 \times 29 \times 31 \times 41 \times 47 \times 59 \times 71$ , que dito em termos de decimais é em torno de  $8 \times 10^{53}$  ou, se preferir, 8 com 53 zeros atrás – um número realmente muito grande. Pode-se mostrar que 20 de 26 grupos esporádicos são representados como subgrupos dentro do “monstro” – os seis grupos que desafiam sistemas classificatórios e são conhecidos como os “seis párias”.

Embora a busca por provas elegantes e breves na matemática seja grande, a prova da classificação de grupos finitos é algo como 10 mil páginas de símbolos estreitamente debatidos. O progresso matemático não é sempre devido ao trabalho de um único gênio proeminente.

## A ideia condensada:



**medida da simetria**

# 39 Matrizes

## linha do tempo

200 a.C.	1850 d.C.	1858	1878	1925
Matemáticos chineses usam agrupamentos de números	J.J. Sylvester introduz o termo "matriz"	Cayley publica a <i>Dissertação sobre a teoria das matrizes</i>	Carl Frobenius prova alguns dos resultados-chave da álgebra das matrizes	Heisenberg usa mecânica de matrizes em teoria quântica

**Esta é a história da “álgebra extraordinária” – uma revolução na matemática que se deu no meio do século XIX. Os matemáticos já brincavam com blocos de números há séculos, mas a ideia de tratar os blocos como um único número decolou há 150 anos com um pequeno grupo de matemáticos que reconheceram seu potencial.**

A álgebra ordinária é a álgebra tradicional, na qual símbolos como  $a$ ,  $b$ ,  $c$ ,  $x$  e  $y$  representam números individuais. Muitas pessoas acham isso difícil de entender, mas para os matemáticos, foi um grande avanço. Em comparação, a “álgebra extraordinária” gerou um abalo sísmico. Para aplicações sofisticadas, esse progresso de uma álgebra unidimensional para uma álgebra multidimensional iria se mostrar incrivelmente poderoso.

**Números multidimensionais** Na álgebra ordinária,  $a$  pode representar um número como 7 e escreveríamos  $a = 7$ , mas na teoria das matrizes, uma matriz  $A$  seria um “número multidimensional”, por exemplo, o bloco

$$A = \begin{pmatrix} 7 & 5 & 0 & 1 \\ 0 & 4 & 3 & 7 \\ 3 & 2 & 0 & 2 \end{pmatrix}$$

Essa matriz tem três linhas e quatro colunas (é uma matriz “3 por 4”), mas em princípio podemos ter matrizes com qualquer número de linhas e colunas – até mesmo uma gigantesca matriz “100 por 200” com 100 linhas e 200 colunas. Uma vantagem crítica da álgebra de matrizes é que podemos pensar em vastos agrupamentos de números, por exemplo um conjunto de dados em estatística, como uma única entidade. Mais do que isso, podemos manipular esses blocos de números simples e eficientemente. Se quisermos somar ou multiplicar todos os números em dois conjuntos de dados, cada um consistindo em mil números, não temos de efetuar mil cálculos – temos de efetuar apenas um (somando ou multiplicando as matrizes).

**Um exemplo prático** Suponhamos que a matriz  $A$  represente a produção da companhia AJAX em uma semana. A companhia AJAX tem três fábricas localizadas em diferentes partes do país e a produção é medida em unidades (digamos milhares de itens) dos quatro produtos que fabricam. No nosso exemplo, as quantidades, correspondendo com a matriz  $A$  na página anterior, são

	Produto 1	Produto 2	Produto 3	Produto 4
Fábrica 1	7	5	0	1
Fábrica 2	0	4	3	7
Fábrica 3	3	2	0	2

Na semana seguinte, a tabela de produção pode ser diferente, mas poderia ser escrita como outra matriz  $B$ . Por exemplo,  $B$  pode ser dada por

$$B = \begin{pmatrix} 9 & 4 & 1 & 0 \\ 0 & 5 & 1 & 8 \\ 4 & 1 & 1 & 0 \end{pmatrix}$$

Qual é a produção total nas duas semanas? O teórico de matrizes diz que é a matriz  $A + B$ , onde os números correspondentes são somados.

Bastante fácil. Infelizmente a matriz de multiplicação é menos evidente.

$$A+B = \begin{pmatrix} 7+9 & 5+4 & 0+1 & 1+0 \\ 0+0 & 4+5 & 3+1 & 7+8 \\ 3+4 & 2+1 & 0+1 & 2+0 \end{pmatrix} = \begin{pmatrix} 16 & 9 & 1 & 1 \\ 0 & 9 & 4 & 15 \\ 7 & 3 & 1 & 2 \end{pmatrix}$$

Voltando à companhia AJAX, suponhamos que os lucros de seus quatro produtos por cada unidade sejam **3, 9, 8, 2**. Certamente podemos computar o lucro total para a fábrica 1 com produções de 7, 5, 0, 1 de seus itens. Funciona como  $7 \times 3 + 5 \times 9 + 0 \times 8 + 1 \times 2 = 68$ .

Mas em vez de lidar com apenas uma fábrica podemos com igual facilidade computar o lucro total  $T$  para *todas* as fábricas.

$$T = \begin{pmatrix} 7 & 5 & 0 & 1 \\ 0 & 4 & 3 & 7 \\ 3 & 2 & 0 & 2 \end{pmatrix} \times \begin{pmatrix} 3 \\ 9 \\ 8 \\ 2 \end{pmatrix} = \begin{pmatrix} 7 \times 3 + 5 \times 9 + 0 \times 8 + 1 \times 2 \\ 0 \times 3 + 4 \times 9 + 3 \times 8 + 7 \times 2 \\ 3 \times 3 + 2 \times 9 + 0 \times 8 + 2 \times 2 \end{pmatrix} = \begin{pmatrix} 68 \\ 74 \\ 31 \end{pmatrix}$$

Olhem cuidadosamente e verão a multiplicação de linha por coluna, uma característica essencial na multiplicação de matrizes. Se além dos lucros das unidades nos dão os volumes das unidades **7, 4, 1, 5** de cada unidade dos produtos, em um só

golpe podemos calcular os lucros e as exigências de armazenamento para as três fábricas pela única multiplicação das matrizes.

$$\begin{pmatrix} 7 & 5 & 0 & 1 \\ 0 & 4 & 3 & 7 \\ 3 & 2 & 0 & 2 \end{pmatrix} \times \begin{pmatrix} 3 & 7 \\ 9 & 4 \\ 8 & 1 \\ 2 & 5 \end{pmatrix} = \begin{pmatrix} 68 & 74 \\ 74 & 54 \\ 31 & 39 \end{pmatrix}$$

O armazenamento total é fornecido pela segunda coluna da matriz resultante, que é 74, 54 e 39. A teoria das matrizes é muito poderosa. Imaginem a situação de uma companhia com centenas de fábricas, milhares de produtos e diferentes exigências de lucros das unidades e capacidade de armazenamento em diferentes semanas. Com a álgebra de matrizes, os cálculos, ou nossa compreensão, ficam razoavelmente imediatos, sem termos de nos preocupar com detalhes que já estão resolvidos.

**Álgebra de matrizes versus álgebra ordinária** Há muitos paralelos entre a álgebra de matrizes e a álgebra ordinária. As diferenças mais famosas ocorrem na multiplicação de matrizes. Se multiplicarmos a matriz  $A$  pela matriz  $B$  e depois tentarmos o contrário:

$$A \times B = \begin{pmatrix} 3 & 5 \\ 2 & 1 \end{pmatrix} \times \begin{pmatrix} 7 & 6 \\ 4 & 8 \end{pmatrix} = \begin{pmatrix} 3 \times 7 + 5 \times 4 & 3 \times 6 + 5 \times 8 \\ 2 \times 7 + 1 \times 4 & 2 \times 6 + 1 \times 8 \end{pmatrix} = \begin{pmatrix} 41 & 58 \\ 18 & 20 \end{pmatrix}$$

$$B \times A = \begin{pmatrix} 7 & 6 \\ 4 & 8 \end{pmatrix} \times \begin{pmatrix} 3 & 5 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 7 \times 3 + 6 \times 2 & 7 \times 5 + 6 \times 1 \\ 4 \times 3 + 8 \times 2 & 4 \times 5 + 8 \times 1 \end{pmatrix} = \begin{pmatrix} 33 & 41 \\ 28 & 28 \end{pmatrix}$$

Então, na álgebra de matrizes podemos ter  $A \times B$  e  $B \times A$  diferentes, uma situação que não existe na álgebra ordinária, em

que a ordem da multiplicação de dois números não altera o resultado.

Outra diferença ocorre com os inversos. Na álgebra ordinária os inversos são fáceis de calcular. Se  $a = 7$ , seu inverso é  $1/7$  porque tem a propriedade  $1/7 \times 7 = 1$ . Algumas vezes escrevemos esse inverso como  $a^{-1} = 1/7$  e temos  $a^{-1} \times a = 1$ .

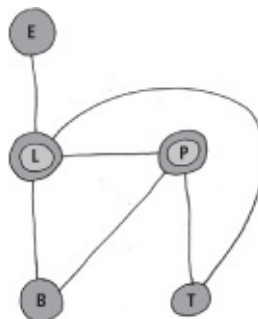
Um exemplo na teoria das matrizes é  $A = \begin{pmatrix} 1 & 2 \\ 3 & 7 \end{pmatrix}$

e podemos verificar que  $A^{-1} = \begin{pmatrix} 7 & -2 \\ -3 & 1 \end{pmatrix}$

porque  $A^{-1} \times A = \begin{pmatrix} 7 & -2 \\ -3 & 1 \end{pmatrix} \times \begin{pmatrix} 1 & 2 \\ 3 & 7 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

onde  $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

é chamada de matriz identidade e é a matriz contrapartida de 1 na álgebra ordinária. Na álgebra ordinária, apenas o 0 não tem um inverso, mas na álgebra das matrizes, diversas matrizes não têm inversos.



**Planos de viagem** Outro exemplo do uso de matrizes é na análise de uma rede de voos de companhias aéreas. Isso vai envolver tanto aeroportos centrais quanto aeroportos secundários. Na prática, pode envolver centenas de destinos – aqui, vamos examinar um pequeno exemplo: os aeroportos centrais de

Londres (L) e Paris (P) e os aeroportos menores de Edimburgo (E), Bordeaux (B) e Toulouse (T) e a rede que mostra os possíveis voos diretos. Para analisar essas redes com um computador, esses aeroportos têm primeiro de ser codificados usando-se matrizes. Se houver um voo direto entre dois aeroportos, um 1 é anotado na intersecção da linha e da coluna marcada por esses aeroportos (como de Londres a Edimburgo). A matriz de “conectividade” que descreve a rede acima é A.

A submatriz mais baixa (marcada pelas linhas pontilhadas) mostra que não há ligações diretas entre os três aeroportos menores. O produto da matriz  $A \times A = A^2$  dessa matriz com ela mesma pode ser interpretado como dando o número de viagens possíveis entre dois aeroportos *com exatamente uma escala*. Então, por exemplo, há 3 possíveis viagens de ida e volta a Paris via outras cidades, mas nenhuma viagem de Londres para Edimburgo que envolva escalas. O número de rotas que são ou diretas ou envolvam escalas são os elementos da matriz  $A + A^2$ . Esse é outro exemplo da capacidade das matrizes de capturar a essência de uma quantidade enorme de dados sob o guarda-chuva de um único cálculo.

$$A \times A = \begin{pmatrix} 4 & 2 & 0 & 1 & 1 \\ 2 & 3 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 2 & 2 \\ 1 & 1 & 1 & 2 & 2 \end{pmatrix}$$

$$A = \begin{matrix} & \begin{matrix} L & P & E & B & T \end{matrix} \\ \begin{matrix} L \\ P \\ E \\ B \\ T \end{matrix} & \begin{pmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \end{pmatrix} \end{matrix}$$

Quando um pequeno grupo de matemáticos criou a teoria das matrizes nos anos 1850, eles o fizeram para resolver problemas de matemática pura. A partir de uma perspectiva aplicada, a teoria das matrizes foi bem o tipo de “solução em busca de um problema”. Como acontece muitas vezes, “problemas” surgiram, que precisavam da teoria nascente. Uma aplicação precoce ocorreu nos anos 1920, quando Werner Heisenberg investigou a “mecânica das matrizes”, uma parte da teoria quântica. Outra pioneira foi Olga Taussky-Todd, que trabalhou durante um período em projeto de aeronaves e usou álgebra de matrizes. Quando perguntada sobre como descobrira o assunto, ela respondeu que foi o contrário, a teoria das matrizes é que a encontrou. Assim é o jogo da matemática.

**A ideia condensada:  
combinando blocos  
de números**



# 40 Códigos

## linha do tempo

55 a.C.	c. 1750 d.C.	1844	Década de 1920	1950	Década de 1970
Julio César invade a Bretanha e usa códigos para se comunicar com seus generais	O teorema de Euler lança os fundamentos da criptografia de chave pública	Morse transmite a primeira mensagem usando seu código	É desenvolvida a máquina Enigma	Richard Hamming publica um artigo-chave sobre códigos com detecção de erro e autocorreção	É desenvolvida a criptografia de chave pública

**O que Júlio César tem em comum com a transmissão de sinais digitais modernos? A resposta imediata é códigos e codificação. A codificação de imagem e de fala em um fluxo de zeros e uns – um código binário – é essencial para enviar sinais digitais para um computador ou aparelho de televisão digital na única linguagem que esses dispositivos entendem. César usou códigos para se comunicar com seus generais e mantinha suas mensagens secretas mudando as letras de sua mensagem de acordo com uma chave que só ele e os generais sabiam.**

A exatidão era essencial para César e também é necessária para a transmissão efetiva dos sinais digitais. César, além disso, queria manter seus códigos secretos do mesmo modo que as companhias de radiodifusão a cabo e por satélite, que querem que apenas assinantes que pagam sejam capazes de decodificar seus sinais.

Vamos primeiro examinar a exatidão. Erro humano, ou “ruído na linha”, sempre pode acontecer. É preciso aceitar isso. O pensamento matemático nos permite construir sistemas de codificação que automaticamente detectam erro e até fazem correções.

**Detecção e correção de erros** Um dos primeiros sistemas de codificação binários foi o código Morse, que usa dois símbolos, pontos  $\cdot$  e traços  $-$ . O inventor norte-americano Samuel F.B. Morse enviou a primeira mensagem interurbana usando esse código de Washington para Baltimore em 1844. Era um código projetado para o telégrafo elétrico de meados do século XIX, sem grande preocupação com um design eficiente. No código Morse, a letra A é codificada como  $\cdot-$ , B como  $- \cdots$ , C como  $- \cdots \cdot$  e outras letras como diferentes sequências de pontos e traços. Um operador de telégrafo enviando “CAB” enviaria a série  $- \cdots \cdot / \cdot - / - \cdots$ . Apesar dos seus méritos, o código Morse não é muito bom em detectar erros, muito menos em corrigi-los. Se o operador de código Morse quisesse enviar “CAB” mas trocasse um ponto por um traço em C, esquecesse o traço em A e ruído na linha substituísse um ponto por um traço em B, o receptor ao receber  $\cdots \cdot / \cdot / - \cdots$  não acharia nada errado e interpretaria a mensagem como “FEZ”.

Em um nível mais primitivo, poderíamos examinar um sistema de codificação consistindo em apenas 0 e 1, onde 0 representa uma palavra e 1, outra. Suponhamos que um comandante de exército tem de transmitir uma mensagem para seus soldados que pode ser ou “invadam” ou “não invadam”. A instrução “invadam” é codificada por “1” e a “não invadam”, por “0”. Se um 1 ou um 0 for incorretamente transmitido o receptor jamais saberá disso – e a instrução errada será dada com consequências desastrosas.

Podemos melhorar as coisas usando palavras de código de comprimento dois. Se dessa vez codificarmos a instrução

“invada” por 11 e a “não invada” por 00 fica melhor. Um erro de um dígito resultaria em receber-se 01 ou 10. Como apenas 11 ou 00 são palavras de código legítimas, o recebedor certamente saberá que foi cometido um erro. A vantagem desse sistema é que um erro seria detectável, mas ainda não saberíamos como corrigi-lo. Se tivesse sido recebido 01, como saberíamos se o enviado teria sido 00 ou 11?

O jeito para um sistema melhor é combinar o projeto com palavras de código mais longas. Se codificarmos a instrução “invada” como 111 e “não invada” como 000, um erro em um dígito certamente seria percebido, como antes. Se soubéssemos que no máximo um erro poderia ter sido cometido (uma suposição razoável, já que a chance de dois erros em uma palavra de código é pequena), a correção poderia na verdade ser feita pelo receptor. Por exemplo, se 110 fosse recebido, então a mensagem correta teria sido 111. Com as nossas regras, não poderia ser 000, já que essa palavra de código está afastada em dois erros de 110. Nesse sistema há apenas duas palavras de código, 000 e 111, mas elas estão afastadas o suficiente para tornar a percepção e a correção do erro possíveis.

O mesmo princípio é usado quando o processamento de palavras está em modo de autocorreção. Se digitarmos “animul”, o processador de palavras detecta o erro e o corrige, adotando a palavra mais próxima, “animal”. Não dá para corrigir inteiramente a linguagem, no entanto, porque se digitarmos “lomp”, não há apenas uma palavra mais próxima; as palavras *lampt*, *limp*, *lump*, *pomp* e *romp* (“lâmpada, flácido, inchaço, pompa e travessura”) são todas equidistantes em termos de

erros únicos de *lomp*.

Um código binário moderno consiste em palavras de código na forma de blocos formados por zeros e uns. A escolha de palavras de código legítimas e suficientemente distantes possibilita tanto a detecção quanto a correção. As palavras de código do código Morse são próximas demais, mas os sistemas de códigos modernos usados para transmitir dados de satélites podem sempre ser postos em modo de autocorreção. Palavras de código longas, com alto desempenho em termos de correção de erros, tomam mais tempo para serem transmitidas, de modo que há uma troca entre comprimento e velocidade de transmissão. Viagens espaciais da NASA já usaram códigos com correção para três erros que se mostraram satisfatórios no combate ao ruído na linha.

**Tornando as mensagens secretas** Júlio César manteve suas mensagens secretas mudando as letras de acordo com uma chave que apenas ele e seus generais sabiam. Se a chave caísse nas mãos erradas, suas mensagens poderiam ser decifradas por seus inimigos. Nos tempos medievais, a rainha Mary da Escócia enviava mensagens secretas em código de sua cela na prisão. O objetivo de Mary era derrubar sua prima, a rainha Elizabeth, mas suas mensagens codificadas foram interceptadas. Mais sofisticada do que o método romano de fazer uma rotação de todas as letras por uma chave, os códigos dela eram baseados em substituições, mas a chave pôde ser descoberta pela análise da frequência das letras e símbolos usados. Durante a Segunda Guerra Mundial, o código alemão Enigma foi decifrado pela descoberta de sua chave. Nesse caso, foi um desafio formidável,

mas o código sempre foi vulnerável porque a chave era transmitida como parte da mensagem.

Um desenvolvimento espantoso na codificação de mensagens foi descoberto nos anos 1970. Correndo de encontro a tudo o que se acreditara anteriormente, dizia que a chave secreta podia ser disseminada para o mundo todo e mesmo assim a mensagem permaneceria em total segurança. Isso é chamado de criptografia de chave pública. O método se baseia num teorema com 200 anos de idade de um ramo da matemática famoso por ser o mais inútil de todos.

**Criptografia de chave pública** O sr. John Sender, um agente secreto conhecido na fraternidade da espionagem como “J”, acaba de chegar à cidade e quer enviar ao seu contato, o dr. Rodney Receiver, uma mensagem secreta para anunciar sua chegada. O que ele faz em seguida é um tanto curioso. Ele vai à biblioteca pública, pega um catálogo telefônico da cidade na prateleira e procura o dr. R. Receiver. No catálogo, encontra dois números ao lado do nome de Receiver – um longo, que é 247, e o outro curto, 5. Essa informação está disponível para todo mundo e é toda a informação de que John Sender precisa para criptografar sua mensagem, que por simplicidade é seu cartão de visita, J. Essa letra é a de número 74 em uma lista de palavras, mais uma vez publicamente disponível.

Sender criptografa 74 calculando  $74^5$  (módulo 247), ou seja, ele quer saber o resto da divisão de  $74^5$  por 247. O cálculo de  $74^5$  pode ser feito em uma calculadora de mão, mas tem de ser feito com exatidão:

$$74^5 = 74 \times 74 \times 74 \times 74 \times 74 = 2.219.006.624$$

e

$$2.219.006.624 = 8.983.832 \times 247 + 120$$

então, dividindo esse número enorme por 247 ele obtém o resto 120. A mensagem criptografada de Sender é 120 e ele transmite isso para Receiver. Como os números 247 e 5 estão publicamente disponíveis, qualquer pessoa poderia criptografar uma mensagem, mas nem todo mundo consegue decifrá-la. O dr. Receiver tem mais informações na manga. Ele inventou seu número pessoal multiplicando dois números primos. Nesse caso, ele obteve o número 247 multiplicando  $p = 13$  e  $q = 19$ , mas só ele sabe isso.

É aqui que o antigo teorema de Leonhard Euler é apanhado e espanado. O dr. Receiver usa o conhecimento de  $p = 13$  e  $q = 19$  para encontrar um valor de  $a$ , onde  $5 \times a = 1$  módulo  $(p - 1)(q - 1)$ , onde o símbolo  $=$  é o sinal de identidade em aritmética modular. Qual é o  $a$ , de modo que dividindo  $5 \times a$  por  $12 \times 18 = 216$  deixa resto 1? Pulando o cálculo todo, ele encontra  $a = 173$ .

Como ele é o único que conhece os números primos  $p$  e  $q$ , o dr. Receiver é o único que pode calcular o número 173. Com isso, ele calcula o resto quando divide o enorme número  $120^{173}$  por 247. Isso está fora da capacidade de uma calculadora manual, mas é facilmente encontrável com o uso de um computador. A resposta é 74, como Euler sabia duzentos anos atrás. Com essa informação, Receiver procura a palavra 74 e vê que J está de volta na cidade.

Você poderá dizer que certamente um *hacker* poderia descobrir o

fato de que  $247 = 13 \times 19$  e o código poderia ser decifrado. Você estaria correto. Mas o princípio de criptografar e decifrar vai ser o mesmo se o dr. Receiver tiver usado outro número em vez de 247. Ele poderia escolher dois números primos muito grandes e multiplicá-los um pelo outro para obter um número muito maior do que 247.

Encontrar dois fatores primos de um número muito grande é praticamente impossível – quais são os fatores de 24.812.789.922.307, por exemplo? Mas números muito maiores do que esse também podiam ser escolhidos. O sistema da chave pública é seguro, e se as potências de supercomputadores unidos conseguirem fatorar um número de criptografia, tudo o que resta ao dr. Receiver fazer é aumentar ainda mais o tamanho do seu número. No fim, é consideravelmente mais fácil para o dr. Receiver “misturar caixas de areia branca com areia preta” do que para qualquer *hacker* separá-las.

**A ideia condensada:  
mantendo as  
mensagens secretas**

# 41 Contagem avançada

## linha do tempo

<b>c.1800 a.C.</b> O papiro Rhind é escrito no Egito	<b>c.1100 d.C.</b> Bhaskara lida com permutações e combinações	<b>1850</b> Kirkman apresenta o problema das 15 colegiais	<b>1930</b> Frank Ramsey trabalha em análise combinatória	<b>1971</b> Ray Chaudhuri prova a existência de sistemas gerais de Kirkman
---	---	--	--	---

O ramo da matemática chamado análise combinatória às vezes é chamado de contagem avançada. Não se trata de somar de cabeça uma coluna de números.

“Quantos?” é uma questão, mas “como os objetos podem ser combinados?”, também. Os problemas são muitas vezes enunciados de modo simples, sem o acompanhamento da pesada superestrutura da teoria matemática – você não precisa conhecer um monte de trabalho preliminar antes de poder arregaçar as mangas. Isso torna os problemas combinatórios atraentes. Mas eles deviam trazer um alerta de saúde: podem viciar e certamente podem causar insônia.

Um conto de St. Ives Crianças podem começar a fazer análise combinatória numa idade bastante precoce. Uma tradicional quadrinha infantil traz uma questão combinatória: *I was going to St. Ives, I met a man with seven wives;*

*Every wife had seven sacks, Every sack had seven cats, Every cat had seven kits.*

*Kits, cats, sacks and wives*

*How many were going to St. Ives?*<sup>[1]</sup>

O último verso é que traz a pegadinha (resposta: uma). Mas qualquer questão sempre pode ser torcida: Quantos vinham de St. Ives? De novo, a interpretação é importante. Podemos ter certeza



de que o homem e suas sete esposas estavam todos saindo de St. Ives? As esposas estavam acompanhando o homem quando ele foi encontrado, ou estavam em algum outro lugar? A primeira exigência para um problema combinatório é que seja claramente enunciado e compreendido.

Vamos supor que o séquito viesse por uma única estrada longe da cidade costeira da Cornualha e que os “gatinhos, gatos, sacos e esposas” estivessem todos presentes. Quantos vinham de St. Ives? A tabela seguinte nos dá uma solução:

homem	1	1
esposas	7	7
sacos	$7 \times 7$	49
gatos	$7 \times 7 \times 7$	343
gatinhos	$7 \times 7 \times 7 \times 7$	<b>2.401</b>
total		<b>2.801</b>

Em 1858, Alexander Rhind, um antiquário escocês, visitava Luxor e deparou-se com um papiro de 5 metros de comprimento, coberto de matemática egípcia datada de 1800 a.C. Comprou-o. Alguns anos mais tarde, o papiro foi adquirido pelo Museu Britânico e seus hieróglifos foram traduzidos. O problema 79 do Papiro Rhind diz respeito a casas, gatos, camundongos e

trigo, muito parecido com o dos gatinhos, gatos, sacos e esposas de St. Ives. Os dois envolvem potências de 7 e o mesmo tipo de análise. A análise combinatória, ao que parece, tem uma longa história.

**Números fatoriais** O problema das filas nos apresenta à primeira arma no arsenal combinatório – o número *fatorial*. Suponhamos que Alan, Brian, Charlotte, David e Ellie formem uma fila E C A B D

com Ellie na ponta da fila, seguida por Charlotte, Alan e Brian, e com David no final. Trocando as pessoas de lugar, outras filas são formadas; quantas filas diferentes são possíveis?

A arte de contar nesse problema depende da escolha. Há 5 escolhas de quem colocamos no primeiro lugar na fila, e uma vez que essa pessoa tenha sido escolhida, há 4 escolhas para a segunda pessoa, e daí por diante. Quando chegamos à última posição, não há escolha alguma, e essa posição só pode ser ocupada pela pessoa que sobrou. Há, portanto,  $5 \times 4 \times 3 \times 2 \times 1 = 120$  filas possíveis. Se começarmos com 6 pessoas, o número de filas diferentes seria  $6 \times 5 \times 4 \times 3 \times 2 \times 1 = 720$ , e para 7 pessoas,  $7 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1 = 5.040$  filas possíveis.

Número	Fatorial
0	1
1	1
2	2
3	6
4	24

$n$	$n!$
5	120
6	720
7	5040
8	40,320
9	362,880

Um número obtido pela multiplicação sucessiva de números inteiros é chamado de fatorial. Ele ocorre com tanta frequência na matemática que é escrito usando a notação  $n!$  (leia-se “ $n$  fatorial”), em vez de  $n \times (n-1) \times (n-2) \times \dots \times 1$ . Vamos dar uma olhada nos primeiros fatoriais (vamos definir  $0!$  como sendo igual a 1). Logo de cara, vemos que configurações bastante “pequenas” dão surgimento a “grandes” números fatoriais. O número  $n$  pode ser pequeno, mas  $n!$  pode ser enorme.

Se ainda estivermos interessados em formar filas de 5 pessoas, mas agora pudermos tirá-las de um grupo de 8 pessoas **A, B, C, D, E, F, G** e **H**, a análise é quase a mesma. Há 8 escolhas para a primeira pessoa na fila, 7 para a segunda, e daí por diante. Mas dessa vez há 4 escolhas para o último lugar. O número de filas possíveis é  $8 \times 7 \times 6 \times 5 \times 4 = 6.720$

Isso pode ser escrito com a notação para números fatoriais, porque  $8 \times 7 \times 6 \times 5 \times 4 = 8 \times 7 \times 6 \times 5 \times 4 \times \frac{3 \times 2 \times 1}{3 \times 2 \times 1} = \frac{8!}{3!}$

**Combinações** A ordem tem importância em uma fila. As duas filas **C E B A D**      **D A C E B**

são feitas com as mesmas letras, mas são filas diferentes. Já

sabemos que podem ser feitas  $5!$  filas com essas letras. Se estivermos interessados em contar os modos de escolher 5 pessoas entre 8 *sem importar* a ordem, temos de dividir  $8 \times 7 \times 6 \times 5 \times 4 = 6.720$  por  $5!$ . O número de modos de se escolher 5 pessoas entre 8 é, portanto,  $\frac{8 \times 7 \times 6 \times 5 \times 4}{5 \times 4 \times 3 \times 2 \times 1} = 56$ .

Esse número, usando C por combinação, é escrito como  ${}^8C_5$  e é  $C_5^8 = \frac{8!}{3!5!} = 56$

Na Loteria Nacional do Reino Unido as regras exigem uma seleção de 6 números entre 49 possíveis – quantas possibilidades há, então?

$$C_6^{49} = \frac{49!}{43!6!} = \frac{49 \times 48 \times 47 \times 46 \times 45 \times 44}{6 \times 5 \times 4 \times 3 \times 2 \times 1} = 13.983.816$$

Só uma combinação ganha, então há aproximadamente 1 chance em 14 milhões de acertar o prêmio.

**Problema de Kirkman** A análise combinatória é um campo amplo e, embora antigo, tem se desenvolvido rapidamente ao longo dos últimos 40 anos em razão de sua relevância para a ciência da computação. Problemas que envolvem teoria dos grafos, quadrados latinos e outros podem ser considerados como fazendo parte da análise combinatória moderna.

A essência da análise combinatória foi capturada por um mestre no assunto, o rev. Thomas Kirkman, trabalhando em uma época em que a análise combinatória era ligada principalmente à matemática recreativa. Ele fez muitas contribuições originais para a geometria discreta, teoria dos grupos e combinatória, mas

nunca foi nomeado para uma universidade. O enigma que reforçou sua fama como um matemático que não perde tempo foi aquela pela qual ele será sempre conhecido. Em 1850, Kirkman apresentou o “problema das 15 colegiais”, no qual estudantes caminham para a igreja em 5 fileiras de 3 todos os dias da semana. Se você está cansado do Sudoku, pode tentar resolver essa. Precisamos organizar um esquema diário, de modo que duas meninas não caminhem juntas mais do que uma vez. Usando minúsculas e maiúsculas deliberadamente, as meninas são **abigail, beatrice, constance, dorothy, emma, frances, grace, Agnes, Bernice, Charlotte, Danielle, Edith, Florence, Gwendolyn e Victoria**, marcadas como **a, b, c, d, e, f, g, A, B, C, D, E, F, G e V**, respectivamente.

Há, na verdade, sete soluções distintas para o problema de Kirkman, e a que daremos é “cíclica” – foi gerada por “trocas de lugar”. É aqui que entra a marcação das meninas.

Segunda			Terça			Quarta			Quinta			Sexta			Sábado			Domingo		
a	A	V	b	B	V	c	C	V	d	D	V	e	E	V	f	F	V	g	G	V
b	E	D	c	F	E	d	G	F	e	A	G	f	B	A	g	C	B	a	D	C
c	B	G	d	C	A	e	D	B	f	E	C	g	F	D	a	G	E	b	A	F
d	f	g	e	g	a	f	a	b	g	b	c	a	c	d	b	d	e	c	e	f
e	F	C	f	G	D	g	A	E	a	B	F	b	C	G	c	D	A	d	E	B

É chamada de cíclica porque, a cada dia, o esquema da caminhada é mudado de **a** para **b**, **b** para **c** até **g** para **a**. O mesmo se aplica para as garotas em maiúsculas **A** para **B**, **B** para **C** e daí por diante, mas Vitória permanece inalterada.

A razão subjacente para a escolha da notação é que as fileiras correspondem a linhas na geometria de Fano (ver p. 117). O

problema de Kirkman não é apenas um jogo de salão; faz parte da matemática corrente.

**A ideia condensada:  
quantas combinações?**

# 42 Quadrados mágicos

## linha do tempo

c.2800 a.C.	c. 1690 d.C.	1693	1770	1988
Nasce a lenda de Lo Shu	de la Loubère produz o método siamês para construir quadrados mágicos	Bernard Frénicle de Bessy enumera os 880 possíveis quadrados mágicos 4 x 4	Euler produz um quadrado elevado ao quadrado	Sallows cria seu quadrado baseado em letras

**“Um matemático”, escreveu G.H. Hardy, “assim como um pintor ou um poeta, é um elaborador de padrões”. Os quadrados mágicos têm padrões bem curiosos, mesmo para critérios matemáticos. Eles ficam no limite entre a matemática cheia de símbolos e os fascinantes modelos adorados pelos fãs de quebra-cabeças.**

$a$	$b$
$c$	$d$

Um quadrado mágico é uma grade quadrada na qual números inteiros distintos são escritos em cada célula da grade, de tal modo que o resultado da soma de cada linha horizontal e de cada coluna vertical, e de cada diagonal, seja o mesmo.

Os quadrados com apenas uma linha e uma coluna são tecnicamente mágicos, mas são muito sem-graça, de modo que vamos esquecê-los. Não existe quadrado mágico com duas linhas e duas colunas. Se houvesse, teria a forma mostrada. Como a soma das linhas e a soma das colunas têm de ser igual, então,  $a + b = a + c$ . Isso significa que  $b = c$ , contrariando o fato de que todos os números têm de ser diferentes.

**O quadrado Lo Shu** Como quadrados de  $2 \times 2$  não existem, vamos

examinar os arranjos  $3 \times 3$  e tentar construir um deles com uma grade. Vamos começar com um quadrado mágico normal, em que a grade é preenchida com os números consecutivos 1, 2, 3, 4, 5, 6, 7, 8, e 9.


Para um quadrado tão pequeno, é possível construir um quadrado mágico  $3 \times 3$  pelo método de “tentativa e teste”, mas podemos primeiro fazer algumas deduções que nos ajudem a avançar. Se somarmos todos os números na grade, teremos  $1 + 2 + 3 + 4 + 5 + 6 + 7 + 8 + 9 = 45$

e esse total terá de ser o mesmo que a soma dos totais de 3 linhas. Isso mostra que cada linha (e coluna e diagonal) precisa somar 15. Agora vamos olhar a célula do meio – vamos chamá-la de  $c$ . Duas diagonais envolvem  $c$  do mesmo modo que a linha do meio e a coluna do meio. Se somarmos os números nessas quatro linhas obtemos  $15 + 15 + 15 + 15 = 60$  e isso deve ser igual a *todos* os números somados, mais 3 lotes extras de  $c$ . A partir da equação  $3c + 45 = 60$ , vemos que  $c$  deve ser 5. Outros fatos podem também ser aprendidos, como não conseguir colocar o 1 numa célula do canto. Com algumas dicas reunidas, estamos em boa posição para usar o método de “tentativa e teste”. Tente!

8	1	6
3	5	7
4	9	2



Uma solução para o quadrado de  $3 \times 3$  pelo método siamês.

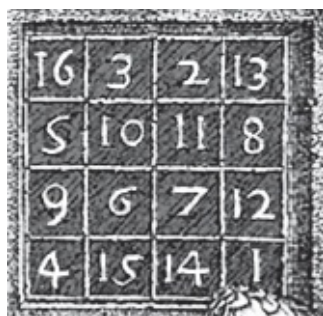
É claro que gostaríamos de ter um método totalmente sistemático para construir quadrados mágicos. Simon de la Loubère, embaixador francês para o rei de Sião no fim do século XVII, encontrou um. Loubère interessou-se por matemática chinesa e escreveu um método para construir quadrados mágicos que tenham um número ímpar de linhas e colunas. Esse método começa colocando o 1 no meio da primeira linha e “subindo e atravessando e rodando, se necessário”, para posicionar o 2 e os números subsequentes. Se bloqueado, é usado o número seguinte abaixo do número atual.

Notavelmente, esse quadrado mágico é essencialmente o único com 3 linhas e 3 colunas. Todos os demais quadrados mágicos  $3 \times 3$  podem ser obtidos a partir desse, rodando-se os números em torno do meio e/ou refletindo números do quadrado na coluna do meio ou na linha do meio. É o chamado quadrado de “Lo Shu” e foi conhecido na China por volta de 3000 a.C. Diz a lenda que ele foi visto pela primeira vez nas costas de uma tartaruga que emergia do rio Lo. As pessoas locais interpretaram isso como um sinal dos deuses de que não ficariam livres de pestilência, a não ser que aumentassem suas oferendas.

Se existe um quadrado mágico  $3 \times 3$ , quantos quadrados mágicos  $4 \times 4$  diferentes existem? A resposta assombrosa é que há 880 (e prepare-se, há 2.202.441.792 quadrados mágicos de ordem 5). Não sabemos quantos quadrados há para valores gerais de  $n$ .

**Quadrados de Dürer e Franklin** O quadrado mágico de Lo Shu é bem conhecido por sua idade e singularidade, mas um quadrado

mágico  $4 \times 4$  se tornou icônico por sua associação com um artista famoso. Além disso, ele tem muito mais propriedades do que o quadrado mágico corriqueiro, que dá 880 versões. Esse é o quadrado mágico  $4 \times 4$  que aparece na gravura *Melancholia* de Albrecht Dürer, feita no ano de 1514.



16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

No quadrado de Dürer, todas as linhas somam 34, do mesmo modo que as colunas, as diagonais e os pequenos quadrados  $2 \times 2$  que compõem o quadrado  $4 \times 4$  completo. Dürer deu um jeito de até “assinar” sua obra-prima com a data do término no meio da linha inferior.

O cientista e diplomata norte-americano Benjamin Franklin reparou que a construção de quadrados mágicos era útil para exercitar a mente. Ele era viciado nisso, e até hoje os matemáticos não têm muita ideia de como ele fazia; grandes quadrados mágicos não podem ser construídos por feliz acaso. Franklin confessou que, em sua juventude, ele gastou muito tempo com esses quadrados, apesar de não gostar muito de “*Arithmetick*” quando menino. Eis aqui um dos que ele descobriu em sua juventude.

52	61	4	13	20	29	36	45
14	3	62	51	46	35	30	19
53	60	5	12	21	28	37	44
11	6	59	54	43	38	27	22
55	58	7	10	23	26	39	42
9	8	57	56	41	40	25	24
50	63	2	15	18	31	34	47
16	1	64	49	48	33	32	17

Nesse quadrado mágico normal, há todo tipo de simetrias. Todas as linhas, colunas e diagonais somam 260, do mesmo modo como as “linhas curvas”, uma das quais nós enfatizamos. Há muitas outras coisas a descobrir – como a soma do quadrado  $2 \times 2$  central mais os quatro boxes dos cantos, que também somam 260. Olhe com cuidado e você vai encontrar um resultado interessante para cada quadrado  $2 \times 2$ .

**Quadrados elevados ao quadrado** Alguns quadrados mágicos podem ter células ocupadas por diferentes números elevados ao quadrado. O problema para a construção desses quadrados foi proposto pelo matemático francês Edouard Lucas em 1876. Até agora nenhum quadrado  $3 \times 3$  ao quadrado foi encontrado, embora um tenha chegado perto.

Todas as linhas e colunas e uma diagonal desse quadrado totalizam a soma mágica de 21.609, mas a outra diagonal falha, já que  $127^2 + 113^2 + 97^2 = 38.307$ . Se você for tentado a encontrar um, você mesmo deve anotar um resultado que já foi provado: o valor da célula central deve ser maior do que  $2,5 \times 10^{25}$ , de modo que não há muito sentido em procurar um quadrado com números pequenos. Isso é matemática séria, que tem ligação com curvas elípticas, usadas para provar o Último Teorema de Fermat. Está provado que não há quadrados mágicos  $3 \times 3$  cujas entradas sejam cubos ou quartas potências.

$127^2$	$46^2$	$58^2$
$2^2$	$113^2$	$94^2$
$74^2$	$82^2$	$97^2$

A busca por quadrados elevados ao quadrado tem, no entanto, tido sucesso para quadrados maiores. Quadrados  $4 \times 4$  e  $5 \times 5$  elevados ao quadrado existem. Em 1770, Euler produziu um exemplo, mas sem mostrar seu método de construção. Famílias inteiras têm desde então sido encontradas ligadas ao estudo da álgebra de quaterniões, os números imaginários tetradimensionais.

**Quadrados mágicos exóticos** Quadrados mágicos grandes podem ter propriedades espetaculares. Uma disposição  $32 \times 32$  foi produzida por um especialista em quadrados mágicos, William Benson, na qual os números, seus quadrados e seus cubos formam todos quadrados mágicos. Em 2001, foi produzido um quadrado de  $1.024 \times 1.024$ , no qual todas as potências dos elementos, até a 5ª, formam quadrados mágicos. Há muitos resultados como esse.

Podemos criar toda uma variedade de outros quadrados mágicos, se as exigências forem relaxadas. Os quadrados mágicos normais estão em voga. Uma variedade de resultados especializados surge, se for retirada a condição de que a soma dos elementos na diagonal tem de ser igual à soma das linhas e das colunas. Podemos procurar quadrados cujos elementos consistem apenas em números primos, ou podemos considerar formatos que não sejam quadrados e que tenham “propriedades mágicas”.

Avançando para dimensões mais altas, somos levados a considerar cubos e hipercubos mágicos.

Mas o prêmio para o quadrado mágico mais notável de todos, certamente no quesito curiosidade, deve ir para o humilde  $3 \times 3$  produzido pelo engenheiro eletrônico e escritor holandês Lee Sallows:

<b>5</b>	<b>22</b>	<b>18</b>
<b>28</b>	<b>15</b>	<b>2</b>
<b>12</b>	<b>8</b>	<b>25</b>

O que há de tão notável nisso? Primeiro escreva o número em palavras (exemplo em inglês):

Five	Twenty-two	Eighteen
Twenty-eight	Fifteen	Two
Twelve	Eight	Twenty-five

Depois conte o número de letras que constitui cada palavra para obter.

<b>4</b>	<b>9</b>	<b>8</b>
----------	----------	----------

<b>11</b>	<b>7</b>	<b>3</b>
<b>6</b>	<b>5</b>	<b>10</b>

Notavelmente esse é um quadrado mágico que consiste nos números consecutivos 3, 4, 5, até 11. Vemos também que o número de letras das somas mágicas dos dois quadrados  $3 \times 3$  (21 e 45) é 9, e adequadamente  $3 \times 3 = 9$ .

**A ideia condensada:  
feitiçaria matemática**

## 43 Quadrados latinos

### linha do tempo

1779 d.C.	1900	1925	1960	1979
Euler explora a teoria dos quadrados latinos	Tarry mostra que não há quadrados latinos ortogonais de ordem 6	Fisher sugere o uso de quadrados latinos para projetar experiências estatísticas	A conjectura de Euler a respeito da não existência de determinados pares de quadrados latinos é refutada por Bose, Parker e Shrikhande	Jogos como o Sudoku são inventados em Nova York

Há alguns anos, o Sudoku vem seduzindo as pessoas. Por todos os lugares, canetas e lápis são mordidos à espera da inspiração certa para o número a ser posto naquele box. Será um 4 ou um 5? Talvez seja 9. Cidadãos a caminho do trabalho saem de seus trens pela manhã tendo feito mais esforço mental do que farão no resto do dia. À noite, o jantar está no forno. É 5, 4, ou seria 7? Todos estão lidando com quadrados latinos – estão sendo matemáticos.

	4		8		3			
		7						3
		9	7			2	6	
3				1		7		9
			6	9	8			
1		5		2				6
	2	3			6	5		
6						1		
			5		2		8	


**Sudoku desvendado** No Sudoku, recebemos uma grade  $9 \times 9$  com alguns números preenchidos. O objetivo é preencher o resto

usando os números dados como dicas. Cada linha e cada coluna deve conter apenas uma vez os algarismos 1, 2, 3..., 9, do mesmo modo que os pequenos quadrados  $3 \times 3$  que o constituem.

Acredita-se que o Sudoku (que significa “algarismos únicos”) foi inventado no fim dos anos 1970. Ganhou popularidade no Japão nos anos 1980, antes de arrebatara a popularidade de massa em 2005. A atração do quebra-cabeça é que, ao contrário de palavras cruzadas, você não precisa ter lido muito para tentá-lo, mas, assim como as palavras cruzadas, ele pode ser instigante. Os viciados nas duas formas de autotortura têm muito em comum.

**Quadrados latinos  $3 \times 3$**  Uma série quadrada contendo exatamente um símbolo em cada linha e cada coluna é chamada de quadrado latino. O número de símbolos é igual ao tamanho do quadrado, e é chamado de “ordem”. Podemos preencher uma grade  $3 \times 3$  em branco, de modo que cada linha e cada coluna contenha exatamente um dos símbolos  $a$ ,  $b$  e  $c$ ? Se pudermos, isso seria um quadrado latino de ordem 3.

Ao introduzir o conceito de quadrado latino, Leonhard Euler chamou-o de um “novo tipo de quadrado mágico”. Ao contrário dos quadrados mágicos, no entanto, os quadrados latinos não estão preocupados com aritmética, e os símbolos não têm de ser números. O motivo para esse nome é simplesmente que os símbolos usados para os formar são tirados do alfabeto latino, enquanto Euler usou o grego, com outros quadrados.

Um quadrado latino  $3 \times 3$  pode ser facilmente anotado.

Se pensamos em  $a$ ,  $b$  e  $c$  como dias da semana, segunda-feira,



quarta-feira e sexta-feira, o quadrado poderia ser usado para agendar reuniões entre duas equipes de pessoal. A Equipe Um é formada por **L**arry, **M**ary e **N**ancy, e a Equipe Dois por **R**oss, **S**ophie e **T**om.

	R	S	T
L	<i>a</i>	<i>b</i>	<i>c</i>
M	<i>b</i>	<i>c</i>	<i>a</i>
N	<i>c</i>	<i>a</i>	<i>b</i>

Por exemplo, **M**ary, da Equipe Um, tem uma reunião com **T**om, da Equipe Dois na segunda-feira (a intersecção da linha **M** com a coluna **T** é *a* – segunda-feira). A disposição do quadrado latino garante que uma reunião aconteça entre cada par de membros da equipe e que não haja coincidência de datas.

Esse não é o único quadrado latino  $3 \times 3$  possível. Se interpretarmos *A*, *B* e *C* como temas discutidos nas reuniões entre Equipe Um e Equipe Dois, podemos produzir um quadrado latino que garante que cada pessoa discuta um tema diferente com um membro da outra equipe.

Então **M**ary da Equipe Um discute o tema *C* com **R**oss, o tema *A* com **S**ophie e o tópico *B* com **T**om.

	R	S	T
L	<i>A</i>	<i>B</i>	<i>C</i>
M	<i>B</i>	<i>C</i>	<i>A</i>
N	<i>C</i>	<i>A</i>	<i>B</i>

Mas quando aconteceriam essas discussões, entre quem e sobre que tema? Qual seria o esquema para essa complexa

organização? Por sorte, os dois quadrados latinos podem ser combinados, símbolo a símbolo, para produzir um quadrado latino composto, no qual cada um dos nove pares possíveis de dias e de tópicos ocorram em exatamente uma posição.

	R	S	T
L	$a, A$	$b, B$	$c, C$
M	$b, B$	$c, C$	$a, A$
N	$c, C$	$a, A$	$b, B$

Outra interpretação para o quadrado é o histórico problema dos “nove oficiais”, no qual nove oficiais pertencentes a três regimentos  $a, b$  e  $c$  e a três postos  $A, B$  e  $C$  são postos no pátio de parada, de modo que cada linha e coluna contenha um oficial de cada regimento e de cada posto. Quadrados latinos que se combinam desse jeito são chamados de “ortogonais”. O caso  $3 \times 3$  é direto, mas encontrar pares de quadrados latinos ortogonais para alguns quadrados maiores não é nada fácil. Isso foi uma coisa que Euler descobriu.

No caso do quadrado latino  $4 \times 4$ , um “problema dos 16 oficiais” seria arrumar as 16 figuras de baralho em um quadrado de modo tal que haja um posto (Ás, Rei, Rainha ou Valete) e um naipe (espadas, paus, copas ou ouros) em cada linha e coluna. Em 1782, Euler propôs o mesmo problema para “36 oficiais”. Em essência, ele estava procurando dois quadrados ortogonais de ordem 6. Não conseguiu encontrá-los e conjecturou que não havia pares de quadrados latinos ortogonais de ordens 6, 10, 14, 18, 22, ... Será que isso poderia ser provado?

Então apareceu Gaston Tarry, um matemático amador que trabalhara como funcionário público na Argélia. Ele examinou exemplos e, por volta de 1900, havia verificado a conjectura de Euler em um caso: não há par de quadrados latinos ortogonais de ordem 6. Os matemáticos naturalmente supuseram que Euler estava correto nos outros casos, 10, 14, 18, 22...

Em 1960, os esforços combinados de três matemáticos assombraram o mundo matemático, provando que Euler estava errado em todos os outros casos. Raj Bose, Ernest Parker e Sharadchandra Shrikhande provavam que havia, mesmo, pares de quadrados latinos ortogonais de ordem 10, 14, 18, 22... O único caso em que quadrados latinos não existem (fora os triviais de ordem 1 e 2) é o de ordem 6.

Vimos que há dois quadrados latinos mutuamente ortogonais de ordem 3. Para a ordem 4, podemos produzir três quadrados que são mutuamente ortogonais, um em relação ao outro. Pode ser mostrado que nunca há mais do que  $n - 1$  quadrados latinos mutuamente ortogonais de ordem  $n$ , então para  $n = 10$ , por exemplo, não poderá haver mais de nove quadrados latinos mutuamente ortogonais. Mas encontrá-los é uma outra história. Até agora ninguém conseguiu sequer produzir três quadrados latinos de ordem 10 que sejam mutuamente ortogonais.

**Os quadrados latinos são úteis?** R.A. Fisher, um eminente estatístico, viu o uso prático para o quadrado latino. Ele os usou para revolucionar métodos agrícolas durante sua época na Estação de Pesquisa de Rothamsted, em Hertfordshire, no Reino Unido.

O objetivo de Fisher era investigar a eficácia de fertilizantes no rendimento de um cultivar. Idealmente, o que se quer é plantar cultivares em condições de solo idênticas, de maneira que a qualidade do solo não seja um fator indesejável que influencie o rendimento do cultivar. Poderíamos então aplicar os diferentes fertilizantes, certos do conhecimento de que a “amolação” da qualidade do solo foi eliminada. O único jeito de garantir condições de solo idênticas seria usar o mesmo solo – mas não é prático ficar cavando e replantando cultivares. Mesmo se isso fosse possível, condições meteorológicas poderiam se tornar um novo estorvo.

Um modo de contornar isso é usar quadrados latinos. Vamos examinar o teste de quatro tratamentos. Se marcamos um campo quadrado em 16 lotes, podemos imaginar o quadrado latino como uma descrição do campo em que a qualidade do solo varia “verticalmente” e “horizontalmente”.

Os quatro fertilizantes são então aplicados aleatoriamente no esquema marcado como  $a$ ,  $b$ ,  $c$  e  $d$ , de modo que exatamente um é aplicado em cada linha e coluna em uma tentativa de eliminar a variação de qualidade do solo. Se suspeitamos que algum outro fator pode influenciar o rendimento do cultivar, podemos lidar com isso também. Suponhamos que achamos que a hora do dia em que o fertilizante é aplicado é um fator. Marque quatro zonas de horas durante o dia como  $A$ ,  $B$ ,  $C$  e  $D$  e use quadrados latinos ortogonais como o projeto para um esquema para reunir dados. Isso garante que cada tratamento e zona horária é aplicado em um dos lotes. O projeto para a experiência seria:

a, hora A	b, hora B	c, hora C	d, hora D
b, hora C	a, hora d	d, hora A	c, hora B
c, hora D	d, hora C	a, hora B	b, hora A
d, hora B	c, hora A	b, hora D	a, hora C

Outros fatores podem ser separados indo adiante e criando projetos de quadrados latinos cada vez mais elaborados. Euler não podia sonhar que a solução do problema dos seus oficiais fosse ser aplicada em experiências agrícolas.

## A ideia condensada:

# sudoku revelado

# 44 Matemática financeira

## linha do tempo

3000 a.C.	1494 d.C.	1718	1756	1848
Os babilônios usam um sistema numérico sexagesimal para negócios financeiros	Luca Pacioli publica tabelas financeiras e um relato de contabilidade de dupla entrada	Abraham de Moivre investiga estatísticas de mortalidade e os fundamentos da teoria das anuidades	James Dodson publica <i>First Lectures on Insurance</i> (Primeiras lições sobre seguros)	É fundado o Instituto dos Atuários em Londres

**Norman é um supervendedor quando se trata de bicicletas. Ele também encara como seu dever fazer com que todos usem bicicleta, de modo que fica encantado quando um cliente vem à sua loja e, sem nenhuma hesitação, compra uma bicicleta por £99. O freguês paga com um cheque de £150, e como os bancos estão fechados, Norman pede ao vizinho que o desconte. Norman volta, dá o troco de £51 ao freguês, que então vai embora em grande velocidade. Segue-se uma calamidade. O cheque volta, o vizinho exige a devolução de seu dinheiro, e Norman agora tem de pedir dinheiro emprestado a um amigo. A bicicleta custou a ele, originalmente, £79, mas quanto Norman perdeu, no total?**

O conceito desse pequeno dilema foi proposto pelo grande elaborador de enigmas Henry Dudeney. É um tipo de matemática financeira, mas mais exatamente é um enigma ligado ao dinheiro. Mostra como o dinheiro depende do tempo e que a inflação vai muito bem, obrigada. Na época em que foi escrito, nos anos 1920, a bicicleta de Dudeney custava na verdade £15 para o consumidor. Uma maneira de combater a inflação é por meio dos juros sobre o dinheiro. Estamos no terreno da matemática séria e do moderno mercado financeiro.

**Juros compostos** Há dois tipos de juros, conhecidos como simples e compostos. Vamos voltar nossos holofotes matemáticos para dois irmãos. Charlie Composto e Simon Simples. O pai dá £1 mil a cada um, que os dois depositam em um banco. Charlie Composto sempre escolhe uma conta que aplica juros compostos, mas Simon Simples é mais tradicional e prefere contas que usam juros simples. Tradicionalmente, o juro composto era identificado com a usura e era malvisto. Hoje em dia, o juro composto é um fato da vida, fundamental para os sistemas monetários modernos. Juros compostos são juros acrescidos de juros, e é por isso que Charlie gosta deles. O juro simples não tem essa característica, e é calculado sobre uma quantia estabelecida, conhecida como o “principal”. Simon pode entender isso facilmente, já que o principal ganha a mesma quantia de juros todos os anos.

$$A = P \times (1 + i)^n$$

Fórmula de juro composto.

Quando se fala de matemática, é sempre bom ter Albert Einstein ao lado – mas a afirmação de que ele teria dito que o juro composto é a maior descoberta de todos os tempos é muito forçada. É inegável que a fórmula do juro composto tem um uso imediato maior do que seu  $E = mc^2$ . Se você economiza dinheiro, toma dinheiro emprestado, usa cartão de crédito, faz uma hipoteca ou compra um plano de previdência privada, a fórmula de juro composto está ao fundo, trabalhando por (ou contra) você. O que os símbolos representam? O termo  $P$  representa



principal (o dinheiro que você economiza ou toma emprestado),  $i$  é a porcentagem da taxa de juros dividida por 100 e  $n$  é o número de períodos de tempo.

Charlie aplica suas £1 mil numa conta que paga 7% de juros anualmente. Quanto ele terá em três anos? Aqui  $P = 1.000$ ,  $i = 0,07$  e  $n = 3$ . O símbolo  $A$  representa a quantia resultante, e pela fórmula dos juros compostos,  $A = £1.225,04$ .

A conta do Simon paga a mesma taxa de juros, 7%, como juro simples. Como seus ganhos se comparam depois de três anos? Pelo primeiro ano ele ganharia £70 de juros e isso seria o mesmo para o segundo e o terceiro anos. Ele teria, portanto,  $3 \times £70$ , resultando em um total de £1.210. O investimento de Charlie foi a melhor decisão de negócio.

Somas de dinheiro que crescem por juros compostos podem aumentar muito rapidamente. Isso é bom se você está economizando, mas não tão bom se está devendo. Um componente-chave no juro composto é o período durante o qual o dinheiro está aplicado. Charlie ouviu falar de um esquema que paga 1% por semana, um *penny* sobre cada libra esterlina. Quanto ele ganharia aplicando nesse esquema?

Simon acha que sabe a resposta: ele sugere que multipliquemos a taxa de juros de 1% por 52 (o número de semanas no ano) para obter uma taxa de porcentagem anual de 52%. Isso significa £520 de juros, fazendo um total de £1.520 na conta. Charlie chama atenção, no entanto, para a mágica do juro composto e a fórmula do juro composto. Com  $P = £1.000$ ,  $i = 0,01$  e  $n = 52$ , Charlie calcula que o acréscimo será  $£1.000 \times (1,01)^{52}$ . Com sua

calculadora ele nota que isso é £1.677,69, muito mais do que o resultado da soma de Simon Simples. O crescimento porcentual equivalente de Charlie é de 67,79%, bem maior do que os 52% calculados por Simon. Simon fica impressionado, mas seu dinheiro já está no banco aplicado a juro simples. Quanto tempo levará para dobrar seus £1.000 originais? A cada ano ele ganha £70 de juros, de modo que tudo o que ele tem de fazer é dividir 1.000 por 70. Isso dá 14,29, de maneira que ele pode ter a certeza de que em 15 anos ele terá mais do que £2.000 no banco. É muito tempo para se esperar. Para mostrar a superioridade do juro composto, Charlie começa a calcular seu próprio período de duplicação. Isso é um pouco mais complicado, mas um amigo conta a ele a respeito da regra do 72.

**A regra de 72** Para uma dada taxa em porcentagem, a regra de 72 é um macete para estimar o número de períodos necessários para que o dinheiro dobre. Embora Charlie esteja interessado em anos, a regra de 72 se aplica a dias ou meses também. Para encontrar o período de duplicação, tudo o que Charlie tem a fazer é dividir 72 pela taxa de juro. O cálculo é  $72/7 = 10,3$ , de modo que Charlie pode relatar a seu irmão que seu investimento vai dobrar em 11 anos, muito mais rápido do que os 15 anos de Simon. A regra é uma aproximação, mas é útil quando se tem de tomar decisões rápidas.

**Valor atual** O pai de Charlie Composto ficou tão impressionado com o bom senso de seu filho que o chama em particular e diz: “proponho lhe dar £100.000”. Charlie fica muito animado. Aí, o pai acrescenta a condição de que só lhe dará os £100.000 quando ele tiver 45 anos, e isso ainda vai demorar 10 anos. Charlie já não

fica tão feliz.

Charlie quer gastar o dinheiro agora, mas é claro que não pode. Ele vai até o banco e promete a eles os £100.000 dentro de dez anos. O banco responde que tempo é dinheiro e que £100.000 em dez anos não é o mesmo que £100.000 agora. O banco tem de calcular qual o tamanho de um investimento que, feito agora, chegue a £100.000 em dez anos. Essa será a quantia que eles emprestarão a Charlie. O banco acredita que uma taxa de crescimento de 12% daria a eles um belo lucro. Qual seria a quantia atual que possa crescer a £100.000 em dez anos com juros de 12%? A fórmula de juro composto pode ser usada também para esse problema. Dessa vez temos  $A = £100.000$  e temos de calcular  $P$ , o valor atual de  $A$ . Com  $n = 10$  e  $i = 0,12$ , o banco estará preparado para adiantar a quantia de  $100.000/(1,12)^{10} = £32.197,32$ . Charlie fica um tanto chocado com um número tão pequeno, mas mesmo assim vai dar para ele comprar aquele Porsche.

$$S = R \times \frac{(1+i)^n - 1}{i}$$

Fórmula de juro composto.

**Como se pode lidar com pagamentos regulares?** Agora que o pai de Charlie prometeu dar £100.000 a seu filho em dez anos, ele precisa economizar dinheiro. Planeja fazer isso com um fluxo de pagamentos iguais a uma caderneta de poupança, feitos ao final de cada ano, durante dez anos. Ao final desse período, ele poderá então entregar o dinheiro a Charlie no dia que prometeu, e

Charlie poderá entregar o dinheiro ao banco para pagar o empréstimo.

O pai de Charlie consegue encontrar uma conta que o permite fazer isso, uma conta que paga uma taxa de juros anual de 8% por todo o período de dez anos. Ele dá a Charlie a tarefa de calcular os pagamentos anuais. Com a fórmula de juro composto, Charlie estava preocupado com um pagamento (o principal original), mas agora ele se preocupa com dez pagamentos feitos em épocas diferentes. Se forem feitos pagamentos regulares  $R$  no fim de cada ano em um ambiente em que a taxa de juro é  $i$ , a quantia economizada depois de  $n$  anos pode ser calculada pela fórmula do pagamento regular.

Charlie sabe que  $S = £100.000$ ,  $n = 10$  e  $i = 0,08$  e calcula que  $R = £6.902,95$ .

Agora que Charlie tem seu Porsche novinho em folha, cortesia do banco, ele precisa de uma garagem para guardá-lo. Resolve financiar  $£300.000$  para comprar uma casa, uma soma de dinheiro que ele pagará em uma série de pagamentos anuais iguais ao longo de 25 anos. Ele reconhece que isso é um problema, no qual  $£300.000$  é o valor presente de uma série de pagamentos a serem feitos, e ele calcula seus pagamentos anuais facilmente. Seu pai fica impressionado e faz ainda mais uso das proezas de Charlie. Ele acaba de receber de aposentadoria uma bolada de  $£150.000$  e quer comprar um plano de previdência com renda anual. “Tudo bem”, diz Charlie, “podemos usar a mesma fórmula, já que a matemática é a mesma. Em vez de o banco imobiliário me adiantar o dinheiro,

que eu pago de volta em prestações regulares, você vai dar a eles o dinheiro e eles vão fazer pagamentos regulares a você”.

Aliás, a resposta para o enigma de Henry Dudeney é £130, ou seja, os £51 que Norman deu ao freguês e os £79 que ele pagou pela bicicleta.

**A ideia condensada:  
juros compostos  
funcionam melhor**

# 45 O problema da dieta

## linha do tempo

1826 d.C.	1902	1945	1947	1984
Fourier antecipa a programação linear; Gauss resolve equações lineares por eliminação	Farkas dá uma solução para sistemas de inequação	Stigler resolve o problema da dieta por método heurístico	Dantzig formula o método simplex e resolve o problema da dieta por programação linear	Karmarkar deriva um novo algoritmo para resolver problemas de programação linear

**Tanya Smith leva sua atividade atlética com grande seriedade. Ela vai à academia todos os dias e monitora de perto sua dieta. Tanya ganha a vida com trabalhos de meio expediente e tem de prestar atenção em para onde o dinheiro vai. É crucial que ela ingira a quantidade correta de sais minerais e vitaminas a cada mês para permanecer em forma e saudável. As quantidades foram determinadas pelo seu técnico. Ele sugere que os futuros campeões olímpicos deveriam ingerir pelo menos 120 miligramas (mg) de vitaminas e pelo menos 880 mg de sais minerais por mês. Para certificar-se de que segue esse regime, Tanya se ampara em dois suplementos alimentares. Um é sob a forma sólida e tem o nome comercial de Solido e o outro é sob forma líquida, comercializado sob o nome de Liquex. O problema dela é decidir quanto de cada deve comprar a cada mês para satisfazer o técnico.**

O problema clássico da dieta é organizar uma nutrição saudável e pagar o menor preço por ela. Foi o protótipo para problemas de programação linear, ramo desenvolvido nos anos 1940 e que é agora usado em uma ampla gama de aplicações.

	Solido	Liquex	Exigências
Vitaminas	2 mg	3 mg	120 mg
Minerais	10 mg	50 mg	880 mg

No início de março, Tanya faz uma visita ao supermercado e procura por Solido e Liquex. Atrás de um pacote de Solido, descobre que ele contém 2 mg de vitaminas e 10 mg de minerais, enquanto uma caixa de Liquex contém 3 mg de vitaminas e 50 mg de minerais. Ela obedientemente enche o carrinho com 30 pacotes de Solido e 5 caixas de Liquex para passar o mês. Enquanto se dirige ao caixa, fica imaginando se tem a quantidade certa. Primeiro calcula quantas vitaminas ela tem no carrinho. Nos 30 pacotes de Solido, ela tem  $2 \times 30 = 60$  mg de vitaminas, e no Liquex,  $3 \times 5 = 15$  mg. No total ela tem  $2 \times 30 + 3 \times 5 = 75$  mg de vitaminas. Repetindo os cálculos para os minerais, ela tem  $10 \times 30 + 50 \times 5 = 550$  mg de minerais.

Como o técnico exigiu que ela tome pelo menos 130 mg de vitaminas e 880 mg de sais minerais, ela precisa de mais pacotes e caixas no carrinho. O problema de Tanya é fazer os malabarismos com as quantidades certas de Solido e Liquex e com as necessidades de vitaminas e sais minerais. Ela volta ao setor de saúde do supermercado e põe mais pacotes e caixas no carrinho. Ela agora tem 40 pacotes e 15 caixas. Com certeza isso estará OK? Ela recalcula e descobre que tem  $2 \times 40 + 3 \times 15 = 125$  mg de vitaminas e  $10 \times 40 + 50 \times 15 = 1.150$  mg de sais minerais. Agora Tanya com certeza satisfaz as recomendações do técnico e chegou até a exceder as quantidades necessárias.

**Soluções factíveis** A combinação (40, 15) de alimentos permitirá a Tanya satisfazer a dieta. Isso é chamado de combinação

possível, ou uma solução “factível”. Já vimos que (30, 5) não é uma solução factível, de modo que existe uma demarcação entre os dois tipos e combinação – soluções factíveis nas quais a dieta é obedecida, e soluções não factíveis, em que não é.

Tanya tem muitas outras soluções. Ela podia encher o carrinho só com Solido. Se fizesse isso, ela teria de comprar pelo menos 88 pacotes. A compra (88, 0) satisfaz as duas necessidades, porque essa combinação conteria  $2 \times 88 + 3 \times 0 = 176$  mg de vitaminas e  $10 \times 88 + 50 \times 0 = 880$  mg de sais minerais. Se comprasse apenas Liquex, ela precisaria, no mínimo, de 40 caixas; a solução factível (0, 40) satisfaz a necessidade tanto de vitaminas quanto de sais minerais, porque  $2 \times 0 + 3 \times 40 = 120$  mg de vitaminas e  $10 \times 0 + 50 \times 40 = 2.000$  mg de sais minerais. Podemos notar que a ingestão de vitaminas e minerais não bate exatamente com qualquer dessas combinações possíveis, embora o técnico vá certamente ficar satisfeito por Tanya estar tendo o suficiente.

**Soluções ideais** Agora o dinheiro entra na situação. Quando Tanya chega ao caixa, precisa pagar por suas compras. Ela nota que os pacotes e as caixas têm o mesmo preço, £5 cada. Das combinações factíveis que encontramos até agora (40, 15), (88, 0) e (0, 40), as contas seriam de £275, £440 e £200, respectivamente, então a melhor solução até agora seria não comprar Solido e comprar 40 caixas de Liquex. Essa seria a compra de menor custo e as necessidades dietéticas seriam alcançadas. Mas a quantidade de comida a comprar não tem sido planejada. Em um impulso, Tanya tentou várias combinações de Solido e Liquex e calculou os custos apenas desses casos. Será



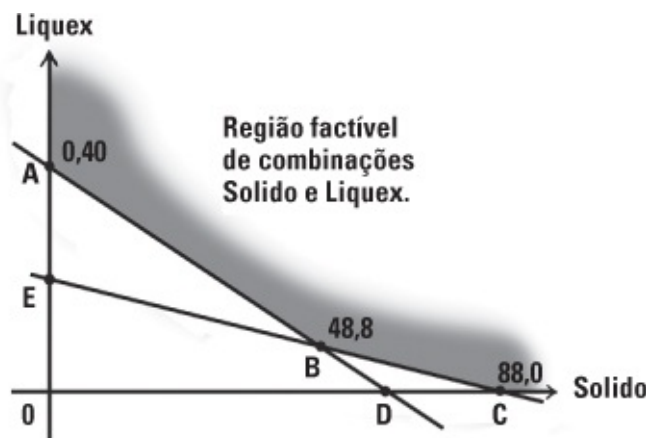
que ela consegue fazer melhor? Haverá uma combinação possível de Solido e Liquex que vá satisfazer seu técnico e ao mesmo tempo custar menos para ela? O que deveria fazer é ir para casa e analisar o problema com lápis e papel.

**Problemas de programação linear** Tanya sempre foi treinada para visualizar suas metas. Se ela pode aplicar isso para ganhar o ouro olímpico, por que não na matemática? Então ela desenha uma imagem da região factível. Isso é possível porque ela está considerando apenas dois alimentos. A linha AD representa as combinações de Solido e Liquex que contêm exatamente 120 mg de vitaminas. As combinações acima dessa linha têm mais do que 120 mg de vitamina. A linha EC representa as combinações que contêm exatamente 880 mg de sais minerais. As combinações de alimentos que estão acima dessas duas linhas constituem a região factível e representam todas as combinações factíveis que Tanya poderia comprar.

Os problemas com a estrutura do problema da dieta são chamados problemas de programação linear. A palavra “programação” significa um procedimento (seu uso antes de se tornar sinônimo de computadores) enquanto “linear” se refere ao uso de linhas retas. Para resolver o problema de Tanya com programação linear, os matemáticos mostraram que tudo de que precisamos é calcular o tamanho da conta de alimentos nos pontos dos ângulos no gráfico de Tanya. Ela descobriu uma nova solução factível no ponto B, com coordenadas (48, 8), o que significa que poderia comprar 48 pacotes de Solido e 8 caixas de Liquex. Se ela fizer isso, vai satisfazer sua dieta *exatamente*, porque nessa combinação há 120 mg de vitaminas e 880 mg de

minerais. A £5 por tanto um pacote quanto uma caixa, essa combinação iria lhe custar £280. Então, a compra ideal permanecerá a mesma que antes, ou seja, ela não deverá comprar nenhum Solido e 40 caixas de Liquex em um custo total de £200, mesmo que venha a ter 1.120 mg de vitaminas a mais do que os 880 mg necessários.

A combinação ideal, no final das contas, vai depender dos custos relativos dos suplementos. Se o custo por pacote de Solido baixar para £2 e o Liquex subir para £7, então as contas para as combinações nos ângulos A (0, 40), B (48, 8) e C (88, 0) seriam respectivamente £280, £152 e £176.



A melhor compra para Tanya, com esses preços, é 48 pacotes de Solido e 8 caixas de Liquex, com uma conta de £152.

**História** Em 1947, o matemático norte-americano George Dantzig, então trabalhando para a Força Aérea dos EUA, formulou um método para resolver problemas de programação linear, chamado método simplex. Teve tanto sucesso que Dantzig se tornou conhecido no Ocidente como o pai da programação linear. Na Rússia soviética, isolada durante a

Guerra Fria, Leonid Kantorovich formulou independentemente uma teoria da programação linear. Em 1975, Kantorovich e o matemático holandês Tjalling Koopman receberam o Prêmio Nobel de Economia por trabalho em alocação de recursos, que incluía técnicas de programação linear.

Tanya levou em conta apenas dois alimentos – duas variáveis –, mas hoje em dia problemas envolvendo milhares de variáveis são corriqueiros. Quando Dantzig encontrou seu método, havia poucos computadores, mas havia o Mathematical Tables Project – uma tarefa de criação que demorou uma década para um esquema que começou em Nova York em 1938. Foi preciso uma equipe de uns dez calculadores humanos trabalhando durante 12 dias com calculadoras de mão para resolver um problema dietético com nove exigências de “vitaminas” e 77 variáveis.

Ao mesmo tempo que o método simplex e suas variantes tiveram um sucesso fenomenal, outros métodos também foram tentados. Em 1984, o matemático indiano Narendra Karmarkar derivou um novo algoritmo de consequência prática, e o russo Leonid Khachiyan propôs um método de importância principalmente teórica.

O modelo de programação linear básico tem sido aplicado a diversas situações que não a de escolher uma dieta. Um tipo de problema, o problema de transporte, trata do transporte de mercadorias de fábricas para depósitos. Tem uma estrutura especial e se tornou um campo em si próprio. O objetivo nesse caso é minimizar o custo do transporte. Em alguns problemas de programação linear, o objetivo é maximizar (como maximizar

lucros). Em outros problemas, as variáveis só aceitam valores inteiros, ou apenas dois valores, 0 e 1, mas esses problemas são bem diferentes e exigem seus próprios procedimentos para a solução.

Resta saber se Tanya Smith ganhará sua medalha de ouro na olimpíada. Se assim for, será mais um triunfo para a programação linear.

**A ideia condensada:  
manter-se saudável  
ao menor custo**

## 46 O caixeiroviajante

### linha do tempo

c. 1810 d.C.	1831	1926	1954	1971	2004
Charles Babbage menciona o problema como sendo interessante	O problema do caixeiro-viajante aparece como um problema prático	Borůvka introduz o algoritmo ganancioso	Dantzig e Dijkstra propõem métodos para atacar o problema do caixeiro-viajante	Cook formula o conceito de $P$ versus $NP$ para algoritmos	David Applegate resolve o problema para todas as 24.978 cidades da Suécia

**James Cook, que vive em Bismarck (Dakota do Norte, EUA) é um excelente caixeiroviajante da empresa Electra, que fabrica limpadores de tapetes. O fato de ele ter sido eleito o caixeiroviajante do ano durante três anos consecutivos é uma prova direta de sua capacidade. Sua área de vendas compreende as cidades de Albuquerque, Chicago, Dallas e El Paso, e uma vez por mês ele faz uma ronda em que visita cada uma delas. A pergunta que ele se faz é como fazer a viagem e ao mesmo tempo minimizar a quilometragem total viajada. É o clássico problema do caixeiroviajante.**

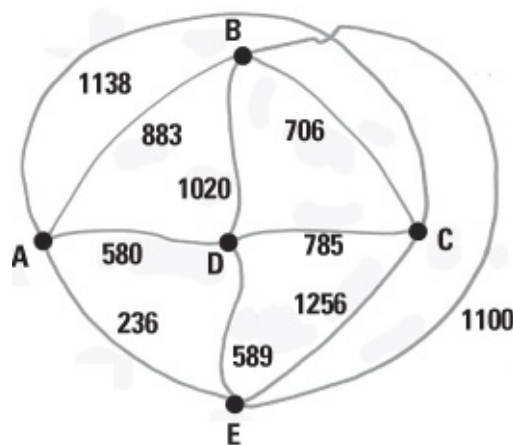
James traçou uma tabela de quilometragens que mostra as distâncias entre as cidades. Por exemplo, a distância entre Bismarck e Dallas é 1.600 km, encontrada na intersecção (sombreada) da coluna Bismarck com a linha Dallas.

**O método ganancioso** Por ser uma pessoa prática, James Cook esboça um mapa da área de vendas, mas não se preocupa com exatidão, desde que o mapa lhe diga aproximadamente onde estão as cidades e qual a distância entre elas. Um trajeto que ele repete muitas vezes começa em Bismarck, vai de lá para Chicago, Albuquerque, Dallas e El Paso, antes de voltar para Bismarck. Esse é o trajeto BCADEB, mas ele se dá conta de que essa viagem de 6.618 km é cara, em termos de distância

percorrida. Será que há um trajeto melhor?

Albuquerque				
1.420	Bismarck			
1.831		Chicago		
933	1.600	1.263	Dallas	
380	1.770	2.021	948	El Paso

Traçar um plano para a área de vendas não deve disfarçar o fato de que James não está com disposição para um planejamento detalhado – ele quer chegar lá e vender. Ao olhar para o mapa em seu escritório em Bismarck, ele vê que a cidade mais próxima é Chicago. São 1.136 km contra os 1.420 km até Albuquerque e 1.770 km até El Paso. Ele começa imediatamente por Chicago, sem um plano geral. Ao chegar a Chicago, termina seus negócios lá e procura a cidade mais próxima. Escolhe Dallas, em vez de Albuquerque e El Paso porque está a 1.263 km de Chicago, e fica mais perto do que as outras opções.



Uma vez em Dallas, ele atingiu  $1.136 + 1.263$  km. Ele então tem de escolher entre Albuquerque e El Paso. Ele escolhe Albuquerque porque é mais perto. De Albuquerque ele tem de ir

até El Paso, onde já terá visitado todas as cidades e, terminada a tarefa, ele volta a Bismarck. Sua quilometragem total é  $1.136 + 1.263 + 933 + 380 + 1.770 = 5.482$ . Esse trajeto BCDAEB é muito mais curto do que o anterior e ele, além disso, economiza nas emissões de carbono.

Esse modo de pensar é muitas vezes chamado de método ganancioso para encontrar uma rota mais curta. Isso porque a decisão de James Cook é sempre local – ele está em uma cidade e procura o melhor trajeto para sair dela. Com esse método, ele nunca tenta olhar adiante mais do que um passo de cada vez. Não é estratégico, porque não leva em conta o resultado geral do melhor trajeto. Por terminar em El Paso, ele teve de fazer um longo trajeto para voltar a Bismarck. OK, ele achou um trajeto mais curto, mas foi mesmo o mais curto? James está intrigado.

James vê um modo de aproveitar o fato de haver apenas cinco cidades envolvidas. Com tão poucas, é possível enumerar todas as rotas possíveis e então escolher a mais curta. Sendo apenas cinco cidades, há apenas 24 trajetos para examinar – ou 12, se considerarmos um trajeto e seu inverso como equivalentes. Isso é permissível porque os dois têm quilometragem igual. O método serve bem a James Cook, e ele fica sabendo que a rota BAEDCB (ou seu inverso BCDEAB) é na verdade a rota ideal, tendo apenas 5.147 km de extensão.

De volta a Bismarck, James percebe que sua viagem demorou demais. Já não é a distância que ele quer economizar, mas o tempo. Ele traça um novo quadro, que dá o tempo de viagem entre as diferentes cidades em seu território.

Quando o problema era a quilometragem, James sabia que a soma das distâncias ao longo de dois lados do triângulo é sempre maior do que o comprimento do terceiro lado; nesse caso, o gráfico é chamado de euclidiano e sabe-se muito a respeito de métodos para as soluções. Esse não é o caso quando o problema é de tempo. Voar nas rotas principais é muitas vezes mais rápido do que nas rotas secundárias, e James Cook nota que ir de El Paso para Chicago é mais rápido do que voar via Dallas. A chamada desigualdade do triângulo não se aplica.

Albuquerque				
12 (terra)	Bismarck			
6 (ar)	2 (ar)	Chicago		
2 (ar)	4 (ar)	3 (ar)	Dallas	
4 (terra)	3 (ar)	5 (ar)	1 (ar)	El Paso

O método ganancioso aplicado ao problema do tempo produz um total de 22 horas na rota BCDEAB, enquanto há dois trajetos ideais distintos, as rotas BCADEB e BCDAEB, cada uma com 14 horas. Dessas rotas, a primeira tem 6.618 km e a segunda, 5.482 km. James Cook fica muito satisfeito porque, ao escolher BCDAEB, ele economizou o máximo. Como projeto futuro, ele pensará no trajeto com o menor custo.

**De segundos a séculos** A verdadeira dificuldade associada ao problema do caixeiroviajante ocorre quando há um grande número de cidades. Como James Cook é um empregado brilhante, rapidamente é promovido a supervisor. Ele agora tem de visitar 13 cidades a partir de Bismarck, em vez das 4 anteriores. Ele não está contente em usar o método ganancioso, e prefere examinar uma listagem completa das rotas. Parte para



enumerar as possíveis rotas para as suas 13 cidades. Logo, descobre que terá  $3,1 \times 10^9$  rotas para examinar. Posto de outra maneira, se um computador levar um segundo para imprimir uma rota, levará cerca de um século para imprimir todas. Um problema que envolva 100 cidades amarraria o computador durante milênios.

Alguns métodos sofisticados têm sido aplicados ao problema do caixeiroviajante. Têm sido dados métodos exatos que se aplicam a 5 mil cidades ou menos, e um foi até bem-sucedido em lidar com um problema particular de 33.810 cidades, embora a potência do computador exigida nesse caso tenha sido colossal. Métodos não exatos produzem trajetos dentro da faixa do ideal com uma probabilidade especificada. Métodos desse tipo têm a vantagem de serem capazes de lidar com problemas com milhões de cidades.

**Complexidade computacional** Olhando para o problema do ponto de vista computacional, vamos pensar no tempo que pode levar para achar uma solução. Simplesmente enumerar todas as rotas possíveis é um cenário de pior caso. James descobriu que esse método de força bruta para 13 cidades demoraria mais de 20 mil anos!

É claro que essas estimativas vão depender do computador usado, mas para  $n$  cidades o tempo tomado aumenta em linha com um  $n$  fatorial (o número que você obtém multiplicando todos os números inteiros de 1 a  $n$ ). Calculamos  $3,1 \times 10^9$  trajetos para 13 cidades. Resolver se cada rota é a mais curta já encontrada se torna um problema de tempo fatorial – e será

muito tempo.

Outros métodos estão disponíveis para atacar o problema, no qual o tempo para  $n$  cidades aumenta com  $2^n$  (2 multiplicado por ele mesmo  $n$  vezes), então para 13 cidades isso envolveria 8.192 decisões (8 vezes mais do que para 10 cidades). Um método dessa complexidade é chamado algoritmo de tempo exponencial. O santo graal desses “problemas de otimização combinatória” é encontrar um algoritmo que dependa não da  $n$ -ésima potência de 2, mas de uma potência fixa de  $n$ . Quanto menor a potência, melhor; por exemplo, se o algoritmo variar de acordo com  $n^2$ , então no caso das 13 cidades isso chegaria a apenas 169 decisões – menos do que duas vezes o tempo tomado por 10 cidades. Diz-se que um método dessa “complexidade” é conduzido em “tempo *polinomial*” – problemas resolvidos desse modo são “problemas rápidos” e podem levar 3 minutos, em vez de séculos.

A classe dos problemas que podem ser resolvidos por um computador em tempo polinomial é representada por  $P$ . Não sabemos se o problema do caixeiroviajante é um desses. Ninguém criou um algoritmo de tempo polinomial para ele, mas tampouco conseguiram mostrar que ele não existe.

Uma classe mais ampla, representada por  $NP$ , consiste em problemas cujas soluções podem ser *verificadas* em tempo polinomial. O problema do caixeiroviajante é definitivamente um desses porque a verificação de que uma *dada* rota é uma distância mais curta do que qualquer distância dada pode ser feita em tempo polinomial. Você simplesmente soma as

distâncias ao longo da rota considerada e as compara com o número dado. *Encontrar* e *verificar* são duas operações diferentes; por exemplo, é fácil verificar que  $167 \times 241 = 40.247$ , mas encontrar os fatores de 40.247 é uma proposta diferente.

Será que *todo* problema que pode ser verificado em tempo polinomial pode ser resolvido em tempo polinomial? Se isso for verdade, as duas classes,  $P$  e  $NP$ , serão idênticas e podemos escrever  $P = NP$ . Uma questão importante para os cientistas computacionais é se  $P = NP$ . Mais da metade deles na profissão acha que isso não é verdade: acreditam que há problemas que podem ser examinados em tempo polinomial, mas que não podem ser resolvidos em tempo polinomial. É um problema tão importante que o Clay Mathematics Institute ofereceu um prêmio de US\$1 milhão para provar se  $P = NP$  ou se  $P \neq NP$ .

**A ideia condensada:  
encontrar o melhor  
trajeto.**

# 47 Teoria dos jogos

## linha do tempo

1713 d.C.	1944	1950	1982	1994
Waldegrave dá a primeira solução matemática para um jogo de dois jogadores	Von Neumann e Morgenstern publicam <i>Teoria dos jogos e comportamento econômico</i>	Tucker apresenta o dilema do prisioneiro e Nash propõe o equilíbrio de Nash	Maynard Smith publica <i>Evolução e a teoria dos jogos</i>	Nash recebe o Prêmio Nobel de Economia por seu trabalho em teoria dos jogos

**Alguns diziam que Johnny era a pessoa mais inteligente viva. John von Neumann era uma criança prodígio que se tornou uma lenda no mundo matemático. Quando se ouviu dizer que ele chegou a uma reunião de táxi, tendo acabado de rabiscar seu “teorema mínimo” da teoria dos jogos, simplesmente acenaram com a cabeça. Era exatamente o tipo de coisa que Neumann fazia. Ele fez contribuições para a mecânica quântica, lógica, álgebra, então por que a teoria dos jogos escaparia de suas vistas? Não escapou – com Oskar Morgenstern, ele escreveu o influente livro *Theory of Games and Economic Behavior* (Teoria dos jogos e comportamento econômico). Num sentido mais amplo, a teoria dos jogos é um tema antigo, mas von Neumann foi a chave para afiar a teoria do “jogo de duas pessoas com soma-zero”.**

**Jogos de duas pessoas com soma-zero** Parece complicado, mas o jogo de duas pessoas com soma-zero é “jogado” por duas pessoas, companhias ou equipes, em que um lado ganha o que o outro lado perder. Se A ganha £200, B perde esses £200; é isso o que significa a soma zero. Não há sentido em A cooperar com B – é pura competição e só há ganhadores ou perdedores. Numa linguagem “ganha-ganha”, A ganha £200 e B ganha -£200 e a soma  $200 + (-200) = 0$ . Essa é a origem do termo “soma-zero”.

Vamos imaginar duas empresas de TV, ATV e BTV, que concorrem para operar um serviço extra de notícias, na Escócia ou na Inglaterra. Cada empresa deve fazer um lance para um único país, e sua decisão será baseada na projeção do aumento do tamanho de suas audiências. Analistas de mídia estimaram o aumento nas audiências e as duas empresas teriam acesso à pesquisa deles. Isso foi convenientemente estabelecido numa “tabela de resultados”, em unidades de um milhão de telespectadores.

Se tanto ATV e BTV resolverem operar na Escócia, então a ATV ganharia 5 milhões de telespectadores, mas a BTV perderia 5 milhões de telespectadores. O significado do sinal de menos, como no resultado -3, é que ATV perderá uma audiência de 3 milhões. Os resultados + são bons para a ATV e os resultados -, bons para a BTV.

Vamos supor que as empresas tomem sua única decisão com base na tabela de resultados e que façam seus lances simultaneamente em propostas seladas. É óbvio que as duas empresas agem de acordo com seus melhores interesses.

		BTV	
		Escócia	Inglaterra
ATV	Escócia	+5	-3
	Inglaterra	+2	+4

Se a ATV escolher a Escócia, o pior que pode acontecer é uma perda de 3 milhões; se apostar na Inglaterra, o pior seria ganhar 2 milhões. A estratégia óbvia para ATV seria escolher a Inglaterra (linha 2). Não faria mal ganhar 2 milhões de

telespectadores, não importando o que BTV escolha. Olhando numericamente, a ATV calcula  $-3$  e  $2$  (os mínimos nas linhas) e escolhe a linha correspondendo ao máximo dessas.

A BTV está em posição mais fraca, mas ainda assim pode calcular uma estratégia que limite suas perdas potenciais e espera uma tabela de lucros melhor no ano seguinte. Se a BTV escolher a Escócia (coluna 1), o pior que poderá ocorrer será uma perda de 5 milhões; se escolher a Inglaterra, o pior será uma perda de 4 milhões. A estratégia mais segura para a BTV seria escolher a Inglaterra (coluna 2), porque perder uma audiência de 4 milhões é preferível a perder 5 milhões. Menos mal perder 4 milhões de telespectadores, não importando o que a ATV decida.

Essas seriam as estratégias mais seguras para cada jogador e, se seguidas, a ATV ganharia mais 4 milhões de telespectadores, enquanto a BTV os perderia.

## Uma mente brilhante

John F. Nash (1928-2015), cuja vida atribulada foi retratada no filme de *Uma mente brilhante*, de 2001, ganhou o Prêmio Nobel de Economia em 1994 por suas contribuições à teoria dos jogos.

Nash e outros estenderam a teoria dos jogos para o caso de mais de dois jogadores e para jogos onde haja cooperação entre os jogadores, inclusive o ataque a um terceiro jogador. O “equilíbrio de Nash” (como o ponto de equilíbrio em uma sela) deu uma perspectiva muito mais ampla do que a estabelecida por von Neumann, resultando numa compreensão maior de situações econômicas.

**Quando um jogo é determinado?** No ano seguinte, as duas empresas de TV tinham mais uma opção – operar no País de Gales. Como as circunstâncias tinham mudado, havia uma nova tabela de resultados.

		BTV		
		País de Gales	Escócia	Inglaterra
ATV	País de Gales	+3	+2	+1
	Escócia	+4	-1	0
	Inglaterra	-3	+5	-2
	Máximo na coluna	+4	+5	+1

Como antes, a estratégia segura da ATV é escolher a linha que maximize o pior que possa acontecer. Então, o máximo de  $\{+1, -1, -3\}$  é escolher o País de Gales (linha 1). A estratégia segura para a BTV é escolher a coluna que minimize de  $\{+4, +5, +1\}$ . É a Inglaterra (coluna 3).

Ao escolher País de Gales, a ATV pode *garantir* o ganho de nada menos que 1 milhão de espectadores, não importando o que a BTV faça, e ao escolher a Inglaterra (coluna 3), a BTV pode garantir que não vai perder mais de 1 milhão de espectadores, não importa o que a ATV faça. Essas escolhas, portanto, representam as melhores estratégias para cada empresa, e nesse sentido o jogo é determinado (mas ainda injusto para a BTV). Nesse jogo

$$\text{máximo de } \{+1, -1, -3\} = \text{mínimo de } \{+4, +5, +1\}$$

e os dois lados da equação têm o valor comum +1. Diferentemente do primeiro jogo, essa versão tem um equilíbrio

“ponto de sela” de +1.

**Jogos repetitivos** O jogo repetitivo icônico é o tradicional jogo de “pedra, papel e tesoura”. Ao contrário do jogo das empresas de TV, que era um jogo único, este é em geral jogado uma meia dúzia de vezes, ou algumas centenas de vezes por competidores nos campeonatos mundiais anuais.

	Papel	Tesoura	Pedra	Mínimo na linha
Papel	Empate = 0	Perde = -1	Ganha = +1	-1
Tesoura	Ganha = +1	Empate = 0	Perde = -1	-1
Pedra	Perde -1	Ganha +1	Empate = 0	-1
Máximo da coluna	+1	+1	+1	

Em “pedra, papel e tesoura”, dois jogadores mostram, cada um, uma mão, dois dedos ou um punho, cada um simbolizando papel, tesoura ou pedra. Eles contam até três e jogam simultaneamente: papel atrai papel, é derrotado por tesoura (já que tesouras cortam papel), mas derrota pedra (porque pode envolver a pedra). No jogo de “papel” as recompensas são, portanto, 0, -1, +1, que é a linha superior da tabela completa das recompensas.

Não há ponto de sela para esse jogo, nem estratégia *pura* e óbvia a ser adotada. Se um jogador sempre escolhe a mesma ação, digamos, papel, o oponente irá detectar isso e simplesmente escolher tesoura para ganhar o tempo todo. Pelo teorema “minimax” de Neumann, há uma “estratégia mista”, ou um jeito de escolher ações diferentes com base em probabilidade.

De acordo com os matemáticos, os jogadores deveriam escolher



aleatoriamente, mas no total as escolhas de papel, tesoura e pedra deveriam cada uma acontecer um terço do tempo. A aleatoriedade “cega” pode não ser sempre o melhor caminho, no entanto, já que campeões mundiais têm meios de escolher sua estratégia com um pouco de viés “psicológico”. Eles são bons em sacar seus oponentes.

**Quando um jogo não é de soma-zero?** Nem todo jogo é de soma-zero – cada jogador tem às vezes sua própria tabela de resultados. Um exemplo famoso é o “dilema do prisioneiro”, projetado por A.W. Tucker.

Duas pessoas, **Andrew** e **Bertie**, são apanhadas pela polícia, suspeitos de um assalto em estrada, e postas em celas separadas para que não possam trocar ideias. As recompensas, nesse caso sentenças criminais, não apenas dependem de suas respostas individuais ao interrogatório da polícia, mas em como eles respondem no conjunto. Se **A** confessa e **B** não, então **A** pega uma sentença de apenas um ano (da tabela de resultados de **A**), mas **B** é condenado a dez anos (da tabela de resultados de **B**). Se **A** não confessar, mas **B**, sim, as sentenças são ao contrário. Se os dois confessarem, pegam quatro anos cada, mas se nenhum confessar e os dois insistirem em sua inocência, eles saem livres!

<b>A</b>		<b>B</b>	
		Confessa	Não confessa
<b>A</b>	Confessa	+4	+1
	Não confessa	+10	0

<b>B</b>		<b>B</b>	
		Confessa	Não confessa
<b>A</b>	Confessa	+4	+10
	Não confessa	+1	0

Se os prisioneiros pudessem cooperar, eles teriam tomado o

curso ideal de ação e não confessar – essa seria uma situação de “ganha-ganha”.

**A ideia condensada:  
matemática do  
ganha-ganha.**

# 48 Relatividade

## linha do tempo

c.1632 d.C.	1676	1687	1881	1887	1905	1915
Galileu dá as "transformações de Galileu" para corpos em queda	Römer calcula a velocidade da luz por meio de observações das luas de Júpiter	Os <i>Principia</i> de Newton descrevem as leis clássicas do movimento	Michelson mede a velocidade da luz com grande exatidão	As transformações de Lorentz são escritas	Einstein publica <i>Sobre a eletrodinâmica de corpos em movimento</i> , o artigo que descreve a relatividade especial	Einstein publica <i>As equações de campo para a gravitação</i> , descrevendo a relatividade geral

**Quando um objeto se move, seu movimento é medido em relação a outros objetos. Se dirigimos ao longo de uma estrada principal a 110 km/h (quilômetros por hora) e outro carro está dirigindo ao nosso lado a 110 km/h na mesma direção, nossa velocidade com relação a esse carro é zero. No entanto, estamos os dois viajando a 110 km/h em relação ao solo. E nossas velocidades são de 220 km/h em relação a um carro que esteja vindo a 110 km/h na pista oposta. A teoria da relatividade mudou esse modo de pensar.**

A teoria da relatividade foi estabelecida pelo físico holandês Hendrik Lorentz no fim do século XIX, mas o avanço definitivo foi feito por Albert Einstein em 1905. O famoso artigo de Einstein sobre a relatividade especial revolucionou o estudo do movimento dos objetos, reduzindo a teoria clássica de Newton, uma façanha magnífica em sua época, a um caso especial.

**De volta a Galileu** Para descrever a teoria da relatividade, tomamos uma dica do próprio mestre: Einstein adorava falar a respeito de trens e de experiências mentais. Em nosso exemplo, Jim Diamond está a bordo de um trem viajando a 95 km/h. Saindo de seu lugar no fim do trem, ele caminha na direção do vagão restaurante a 3 km/h. Sua velocidade é de 98 km/h em

relação ao solo. Ao voltar para seu assento, a velocidade relativa de Jim em relação ao solo será de 92 km/h, porque ele está andando na direção oposta à do trajeto do trem. Isso é o que a teoria de Newton nos diz. A velocidade é um conceito relativo, e a direção do movimento de Jim determina se você soma ou subtrai.

Como todo movimento é relativo, falamos de um “ponto de referência” como sendo o ponto de vista a partir do qual um movimento em particular é medido. No movimento unidimensional do trem que se movimenta ao longo de um trilho reto, podemos pensar num ponto de referência fixo posicionado na estação ferroviária a uma distância  $x$  e um tempo  $t$  em termos desse ponto de referência. A posição zero é determinada por um ponto marcado na plataforma e o tempo é lido no relógio da estação. As coordenadas distância/tempo relativas a esse ponto de referência na estação são  $(x, t)$ .

Há também um ponto de referência a bordo do trem. Se medirmos a distância até o final do trem e medirmos o tempo pelo relógio do Jim, haverá um outro conjunto de coordenadas,  $(\bar{x}, \bar{t})$ . É também possível sincronizar esses dois sistemas de coordenadas. Quando o trem passa pela marca na plataforma, então  $-x = 0$  e o relógio da estação está em  $t = 0$ . Se Jim estabelecer  $\bar{x} = 0$  nesse ponto, e puser  $\bar{t} = 0$  em seu relógio, há agora uma conexão entre essas coordenadas.

No momento em que o trem passa pela estação, Jim vai para o vagão-restaurant. Podemos calcular a que distância ele está da estação depois de cinco minutos. Sabemos que o trem está se

movimentando a 1,6 km por minuto, então nesse momento ele viajou oito quilômetros, e Jim caminhou  $\bar{x} = 16/60$  de um quilômetro (de sua velocidade de 3,2 km/h multiplicada pelo tempo 8/60). Então, no total Jim está a uma distância ( $x$ ), que é 8 16/60 quilômetros da estação. A relação entre  $x$  e  $\bar{x}$  é, portanto, dada por  $x = \bar{x} + v \times t$  (onde  $v = 60$ ). Rearranjando a equação para dar a distância que Jim caminhou, relativa ao ponto de referência no trem, obtemos

$$\bar{x} = x - v \times t$$

O conceito de tempo na teoria newtoniana clássica é um fluxo unidimensional do passado para o futuro. É universal para todos e independe do espaço. Como é uma quantidade absoluta, o tempo de Jim a bordo do trem é o mesmo que para o mestre da estação na plataforma,  $t$ , então

$$\bar{t} = t$$

Essas duas fórmulas para  $\bar{x}$  e  $\bar{t}$ , derivadas pela primeira vez por Galileu, são tipos de equações chamadas transformações, já que elas transformam quantidades de um ponto de referência para outro. De acordo com a teoria clássica de Newton, seria preciso esperar que a velocidade da luz obedecesse a essas duas transformações galileanas para  $\bar{x}$  e  $\bar{t}$ .

$$\alpha = \frac{1}{\sqrt{1 - \frac{v^2}{c^2}}}$$

## O fator de Lorentz

No século XVII, as pessoas reconheceram que a luz tinha velocidade, e seu valor aproximado foi medido em 1767 pelo astrônomo dinamarquês Ole Römer. Quando Albert Michelson mediu a velocidade da luz com maior exatidão em 1881, ele encontrou 300 mil km por segundo. Mais do que isso, ele percebeu que a transmissão da luz era muito diferente da transmissão do som. Michelson descobriu que, diferentemente da velocidade do nosso observador num trem em movimento, a direção do raio de luz não tem nenhuma relação com a velocidade da luz. Esse resultado paradoxal tinha de ser explicado.

**A teoria especial da relatividade** Lorentz estabeleceu as equações matemáticas que governavam a ligação entre distância e tempo quando um ponto de referência se move a uma velocidade constante  $v$  relativa a outro ponto. Essas transformações eram muito parecidas com as que já calculamos, mas envolvem um fator (de Lorentz) que depende de  $v$  e da velocidade da luz,  $c$ .

**Entra Einstein** A maneira como Einstein lidou com a descoberta de Michelson a respeito da velocidade da luz foi adotá-la como postulado:

A velocidade da luz tem o mesmo valor para todos os observadores e independe da direção.

Se Jim Diamond piscasse uma lanterna, ligando e desligando, enquanto estivesse passando pela estação em seu trem em movimento, apontando o feixe de luz pelo vagão na direção do

avanço do trem, ele mediria sua velocidade como  $c$ . O postulado de Einstein diz que o mestre da estação, observando na plataforma, também mediria a velocidade do feixe de luz como  $c$ , não como  $c + 95 \text{ km/h}$ . Einstein, além disso, supôs um segundo princípio:

*Um ponto de referência se move com velocidade constante em relação a outro.*

O triunfo do artigo de Einstein de 1905 foi devido, em parte, ao modo como ele abordou seu trabalho, motivado pela elegância matemática. Ondas sonoras viajam com vibrações de moléculas no meio em que o som está sendo levado. Outros físicos supuseram que a luz também precisava de algum meio sobre o qual viajar. Ninguém sabia o que era, mas deram um nome a esse meio – o éter luminífero.

Einstein não teve necessidade de supor a existência do éter como meio de transmissão de luz. Em vez disso, ele deduziu as transformações de Lorentz a partir de dois princípios simples de relatividade e a teoria inteira se desenvolveu. Em particular, ele mostrou que a energia de uma partícula  $E$  é determinada pela equação  $E = mc^2$ .

Para a energia de um corpo em repouso (quando  $v = 0$  e, portanto,  $\alpha = 1$ ), isso leva à icônica equação mostrando que massa e energia são equivalentes:

$$E = mc^2$$

Tanto Lorentz quanto Einstein foram considerados para o Prêmio Nobel em 1912. Lorentz já o tinha recebido em 1902, mas

Einstein precisou esperar até 1921, quando finalmente concederam a ele o prêmio pelo trabalho sobre o efeito fotoelétrico (que ele também já tinha publicado em 1905). Aquele foi um ano e tanto para o funcionário de patentes na Suíça.

**Einstein versus Newton** Para a observação em trens em baixa velocidade, há pouca diferença entre a teoria da relatividade de Einstein e a teoria clássica de Newton. Nessas situações, a velocidade relativa  $v$  é tão pequena, quando comparada com a velocidade da luz, que o fator de Lorentz  $\alpha$  é quase 1. Nesse caso, as equações de Lorentz são praticamente as mesmas que as clássicas transformações galileanas. Então, para velocidades baixas, Einstein e Newton concordariam um com o outro. Velocidades e distâncias têm de ser muito grandes para que as diferenças entre as duas teorias fiquem aparentes. Até o trem TGV francês, que quebrou recordes, não chegou ainda a essas velocidades, e ainda vai demorar muito no desenvolvimento das viagens de trem antes que tenhamos de descartar a teoria de Newton em favor da de Einstein. As viagens espaciais nos obrigarão a ir com Einstein.

**A teoria geral da relatividade** Einstein publicou sua teoria geral em 1915. Essa teoria se aplica ao movimento quando os pontos de referência podem se acelerar em relação uns aos outros e ligam os efeitos da aceleração aos da gravidade.

Einstein foi capaz de prever fenômenos físicos tais como a deflexão de feixes de luz por campos gravitacionais de grandes objetos, como o Sol, pelo uso da teoria geral. Sua teoria explicou também o movimento do eixo de rotação de Mercúrio. Essa



precessão não podia ser explicada plenamente pela teoria gravitacional de Newton e pela força exercida sobre Mercúrio pelos outros planetas. Foi um problema que intrigou os astrônomos desde os anos 1840.

O ponto de referência apropriado para a teoria geral é o do espaço-tempo tetradimensional. O espaço euclidiano é chato (tem curvatura zero), mas a geometria espaço-tempo tetradimensional de Einstein (ou geometria riemanniana) é curva. Ela toma o lugar da força de gravidade newtoniana como explicação para objetos que são atraídos uns pelos outros. Com a teoria geral da relatividade de Einstein, é a curvatura do espaço-tempo que explica essa atração. Em 1915, Einstein lançou outra revolução científica.

**A ideia condensada:  
a velocidade da  
luz é absoluta**

# 49 O último teorema de Fermat

## linha do tempo

1665 d.C.	1753	1825	1839	1843	1907	1908	1994
Fermat morre sem deixar registros de sua "prova maravilhosa"	Euler prova o caso para $n = 3$	Legendre e Dirichle independentemente provam o caso para $n = 5$	Lamé prova o caso para $n = 7$	Kummer alega que provou o teorema, mas Dirichlet expõe uma falha	Von Lindemann alega uma prova, mas ela se revela estar errada	Wolfskehl oferece um prêmio para quem a solucionasse dentro de 100 anos	Wiles finalmente prova o teorema

**Podemos somar dois números quadrados para fazer um terceiro quadrado. Por exemplo,  $5^2 + 12^2 = 13^2$ . Mas será que podemos somar dois números ao cubo para formar um outro cubo? E as potências mais altas?**

**Notavelmente, não podemos. O último teorema de Fermat diz que, para quaisquer quatro números inteiros,  $x, y, z$  e  $n$ , não há solução para a equação  $x^n + y^n = z^n$  quando  $n$  é maior do que 2. Fermat alegou ter encontrado uma “prova maravilhosa”, torturando as gerações de matemáticos que se seguiram, inclusive um garoto de 10 anos que leu a respeito dessa caça ao tesouro matemático um dia, em sua biblioteca local.**

O último teorema de Fermat trata de uma equação diofantina, o tipo de equação que impõe os mais duros de todos os desafios. Essas equações exigem que suas soluções sejam números inteiros. Receberam o nome de Diofanto de Alexandria, cuja *Arithmetica* se tornou um marco na teoria dos números. Pierre de Fermat era advogado e funcionário público no século XVII em Toulouse, na França. Matemático versátil, ele gozava de uma alta reputação na teoria dos números, e é mais notavelmente lembrado pela afirmativa de seu último teorema, sua contribuição final à matemática. Fermat o provou, ou pensou que provou, e escreveu em seu exemplar da *Arithmetica* de

Diofanto: “Descobri uma prova verdadeiramente maravilhosa, mas a margem é pequena demais para contê-la”.

Fermat resolveu muitos problemas extraordinários, mas parece que o último teorema de Fermat não foi um deles. O teorema ocupou legiões de matemáticos durante trezentos anos, e só foi provado recentemente. Essa prova não pode ser escrita em margem alguma e as técnicas modernas exigidas para gerá-la lançaram dúvidas extremas sobre a alegação de Fermat.

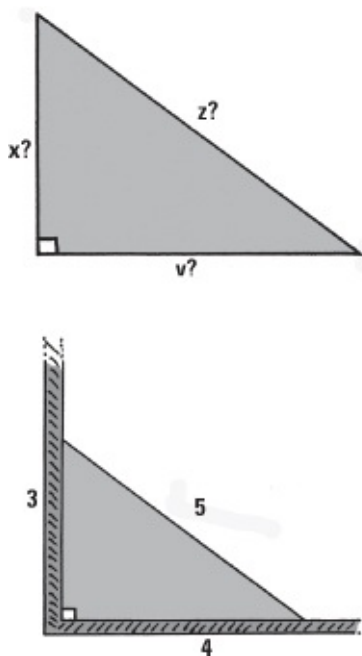
**A equação  $x + y = z$**  Como podemos resolver essa equação de três variáveis  $x$ ,  $y$  e  $z$ ? Em geral, uma equação tem uma incógnita  $x$ , mas aqui temos três. Na verdade, isso faz com que a equação  $x + y = z$  seja bastante fácil de resolver. Podemos escolher os valores de  $x$  e  $y$  do jeito que quisermos, somá-los para obter  $z$  e esses três valores resultarão em uma solução. Simples assim.

Por exemplo, se escolhemos  $x = 3$  e  $y = 7$ , os valores  $x = 3$ ,  $y = 7$  e  $z = 10$  dão o resultado da equação. Podemos também ver que alguns valores de  $x$ ,  $y$  e  $z$  não são soluções para a equação. Por exemplo,  $x = 3$ ,  $y = 7$  e  $z = 9$  não são uma solução porque esses valores não tornam o lado esquerdo da equação  $x + y$  igual ao lado direito,  $z$ .

**A equação  $x^2 + y^2 = z^2$**  Agora vamos pensar nos quadrados. O quadrado de um número é aquele número multiplicado por ele mesmo, o número que escrevemos como  $x^2$ . Se  $x = 3$ , então  $x^2 = 3 \times 3 = 9$ . A equação em que estamos pensando agora não é  $x + y = z$ , mas

$$x^2 + y^2 = z^2$$

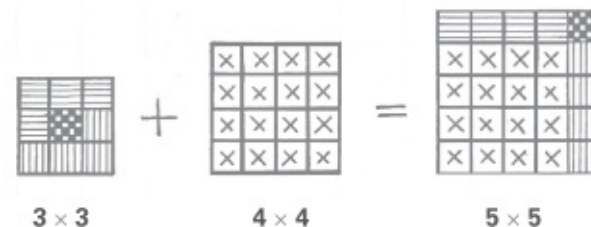
será que podemos resolver isso como antes, escolhendo valores para  $x$  e  $y$  e calculando o  $z$ ? Com os valores  $x = 3$  e  $y = 7$ , por exemplo, o lado esquerdo da equação é  $3^2 + 7^2$ , que é  $9 + 49 = 58$ . Para isso, o  $z$  teria de ser a raiz quadrada de 58 ( $z = \sqrt{58}$ ) que é cerca de 7,6158. Certamente temos o direito de alegar que  $x = 3$ ,  $y = 7$  e  $z = \sqrt{58}$  é uma solução para  $x^2 + y^2 = z^2$ , mas infelizmente as equações diofantinas estão preocupadas sobretudo com soluções em números inteiros. Como  $\sqrt{58}$  não é um número inteiro, a solução  $x = 3$ ,  $y = 7$  e  $z = \sqrt{58}$  não vai servir.



A equação  $x^2 + y^2 = z^2$  é ligada a triângulos. Se  $x$ ,  $y$  e  $z$  representam os comprimentos dos três lados de um triângulo retângulo, eles satisfazem a equação. Inversamente, se  $x$ ,  $y$  e  $z$  satisfazem a equação, então o ângulo entre  $x$  e  $y$  é um ângulo reto. Por causa da conexão com o teorema de Pitágoras, as soluções para  $x$ ,  $y$  e  $z$  são chamadas de triplos pitagóricos.

Como podemos encontrar triplos pitagóricos? É aí que o

construtor local vem em socorro. Parte do equipamento dos construtores é o onipresente triângulo 3-4-5. Os valores  $x = 3$ ,  $y = 4$  e  $z = 5$  acabam sendo a solução do tipo que estamos buscando porque  $3^2 + 4^2 = 9 + 16 = 25 = 5^2$ . Pela recíproca, um triângulo com dimensões 3, 4 e 5 tem de incluir um ângulo reto. Esse é o fato matemático que o construtor usa para erguer suas paredes em ângulos retos.



Nesse caso, podemos quebrar um quadrado de  $3 \times 3$  e envolvê-lo em torno de um quadrado  $4 \times 4$  para fazer um quadrado  $5 \times 5$ .

Há outras soluções de números inteiros para  $x^2 + y^2 = z^2$ . Por exemplo,  $x = 5$ ,  $y = 12$  e  $z = 13$  é outra solução, porque  $5^2 + 12^2 = 13^2$ , e de fato há um número infinito de soluções para a equação. A solução do construtor,  $x = 3$ ,  $y = 4$  e  $z = 5$ , tem uma posição privilegiada porque é a menor solução, e é a única solução composta de números inteiros consecutivos. Há muitas soluções em que dois números são consecutivos, como  $x = 20$ ,  $y = 21$  e  $z = 29$ , além de  $x = 9$ ,  $y = 40$  e  $z = 41$ , mas fora  $x = 3$ ,  $y = 4$  e  $z = 5$ , nenhuma outra tem três.

**Do banquete à fome** Parece um passo pequeno, ir de  $x^2 + y^2 = z^2$  para  $x^3 + y^3 = z^3$ . Desse modo, seguindo a ideia de rearrumar um quadrado em torno de outro para formar um terceiro quadrado, será que podemos fazer o mesmo truque com um cubo? Será que é possível rearranjar um cubo em torno de outro para formar um

terceiro? Acontece que isso não pode ser feito. A equação  $x^2 + y^2 = z^2$  tem um número infinito de soluções diferentes, mas Fermat não conseguiu encontrar sequer um exemplo com número inteiro para  $x^3 + y^3 = z^3$ . O pior estava por vir, e o fato de Leonhard Euler não ter encontrado exemplo algum o levou a exprimir o último teorema:

*Não há solução em números inteiros para a equação  $x^n + y^n = z^n$  para qualquer valor mais alto do que 2.*

Um jeito de abordar o problema de provar que isso é verdadeiro é começar com valores baixos de  $n$  e ir subindo. Foi assim que Fermat trabalhou. O caso  $n = 4$  é na verdade mais simples do que  $n = 3$ , e é provável que Fermat tivesse uma prova para esse caso. Nos séculos XVIII e XIX, Euler preencheu o caso de  $n = 3$ , Adrien-Marie Legendre completou o caso de  $n = 5$  e Gabriel Lamé provou o caso  $n = 7$ . Lamé inicialmente achou que tinha uma prova para o teorema geral, mas infelizmente estava enganado.

Ernst Kummer foi um grande contribuidor e, em 1843, apresentou um manuscrito alegando ter provado o teorema em geral, mas Dirichlet apontou uma falha no argumento. A Academia Francesa de Ciências ofereceu um prêmio de 3 mil francos por uma prova válida, acabando por concedê-lo a Kummer por sua meritória tentativa. Kummer provou o teorema para todos os primos menores do que 100 (e outros valores), mas excluiu os primos irregulares 37, 59 e 67. Por exemplo, ele não conseguiu provar a existência de números inteiros que satisfizessem  $x^{67} + y^{67} = z^{67}$ . Seu fracasso em provar o teorema

em geral serviu para esclarecer técnicas valiosas em álgebra abstrata. Isso talvez tenha sido uma contribuição maior para a matemática do que resolver a equação propriamente dita.

Ferdinand von Lindemann, que provou que o círculo não podia ser em forma de quadrado (ver p. 24), alegou ter provado o teorema em 1907, mas viu-se que estava errado. Em 1908, Paul Wolfskehl deixou um prêmio de 100 mil marcos, válido por 100 anos, a ser concedido ao primeiro que fornecesse uma prova. Ao longo dos anos, algo como 5 mil provas foram submetidas, examinadas, e devolvidas aos esperançosos como sendo falsas.

**A prova** Embora a ligação com o teorema de Pitágoras só se aplique para  $n = 2$ , a ligação com a geometria acabou sendo a chave para sua prova conclusiva. A conexão foi feita com a teoria das curvas e uma conjectura apresentada por dois matemáticos japoneses, Yutaka Taniyama e Goro Shimura. Em 1993, Andrew Wiles deu uma palestra sobre essa teoria em Cambridge e incluiu sua prova do teorema de Fermat. Infelizmente, a prova estava errada.

Um matemático francês com nome parecido, André Weil, descartou essas tentativas. Ele comparou provar o teorema com subir o Everest, e acrescentou que se faltou a alguém 100 metros para chegar ao topo, ele não subiu o Everest. A pressão continuava. Wiles se isolou e trabalhou no problema incessantemente. Muitos pensaram que Wiles iria se unir àquela multidão dos “quase”.

Com a ajuda de colegas, no entanto, Wiles conseguiu eliminar o erro e substituí-lo por um argumento correto. Dessa vez, ele

convenceu os especialistas e provou o teorema. Sua prova foi publicada em 1995 e ele reivindicou o prêmio Wolfskehl justo dentro do período que o qualificaria como uma celebridade matemática. O garoto de dez anos sentado em uma biblioteca pública lendo a respeito do problema anos antes percorreu um longo caminho.

## **A ideia condensada: provando um ponto periférico**



# 50 Hipótese de Riemann

## linha do tempo

1854 d.C.	1859	1896	1900	1914	2004
Riemann começa seu trabalho sobre a função zeta	Riemann prova que as soluções-chave ficam em uma faixa crítica e apresenta sua conjectura	De la Vallée-Poussin e Hadamard mostram que todos os zeros importantes ficam dentro da faixa crítica de Riemann	Hilbert põe a hipótese em sua lista de problemas críticos para os matemáticos resolverem	Hardy prova que há um número infinito de soluções ao longo da linha de Riemann	Verifica-se que os primeiros 10 trilhões de zeros ficam na linha crítica

**A hipótese de Riemann representa um dos desafios mais instigantes na matemática pura. A conjectura de Poincaré e o último teorema de Fermat foram resolvidos, mas a hipótese de Riemann, não. Uma vez decididas, de um jeito ou de outro, questões evasivas a respeito da distribuição de números primos serão resolvidas e os matemáticos poderão ponderar acerca de uma série de novas questões em aberto.**

A história começa com a soma de frações do tipo

$$1 + \frac{1}{2} + \frac{1}{3}$$

A resposta é  $15/6$  (aproximadamente 1,83). Mas o que acontece se continuarmos somando frações cada vez menores, digamos, até dez delas?

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8} + \frac{1}{9} + \frac{1}{10}$$

Usando apenas uma calculadora de mão, a soma dessas frações é aproximadamente 2,9 em decimais. Uma tabela mostra como o total cresce à medida que se acrescentam mais termos.

A série de números

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \dots$$

é chamada de série harmônica. A classificação “harmônica” tem origem nos pitagóricos, que acreditavam que uma corda musical dividida ao meio, um terço, um quarto, daria as notas essenciais para a harmonia.

Número de termos	Total (aproximado)
<b>1</b>	<b>1</b>
<b>10</b>	<b>2,9</b>
<b>100</b>	<b>5,2</b>
<b>1,000</b>	<b>7,5</b>
<b>10,000</b>	<b>9,8</b>
<b>100,000</b>	<b>12,1</b>
<b>1.000.000</b>	<b>14,4</b>

<b>1,000,000,000</b>	<b>21,3</b>

Nas séries harmônicas, frações cada vez menores estavam sendo acrescentadas, mas o que acontece com o total? Será que ele cresce além de todos os números, ou existe uma barreira em algum lugar, um limite acima do qual ela nunca vai? Para responder isso, o truque é agrupar os termos, dobrando a série à medida que avançamos. Se somarmos os primeiros 8 termos, (reconhecendo que  $8 = 2 \times 2 \times 2 = 2^3$ ) por exemplo.

$$S_{2^3} = 1 + \frac{1}{2} + \left(\frac{1}{3} + \frac{1}{4}\right) + \left(\frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8}\right)$$

(onde S representa soma) e, como  $1/3$  é maior do que  $1/4$  e  $1/5$  é maior do que  $1/8$  (e daí por diante), essa soma é maior do que

$$1 + \frac{1}{2} + \left(\frac{1}{4} + \frac{1}{4}\right) + \left(\frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8}\right) = 1 + \frac{1}{2} + \frac{1}{2} + \frac{1}{2}$$

Então, podemos dizer que

$$S_{2^3} > 1 + \frac{3}{2}$$

E mais geralmente

$$S_{2^k} > 1 + \frac{k}{2}$$

Se fizermos  $k = 20$ , de modo que  $n = 2^{20} = 1.048.576$  (mais de um milhão de termos), a soma da série terá apenas excedido 11 (ver

tabela). Está aumentando de um jeito dolorosamente lento – mas pode-se escolher um valor para  $k$ , de modo que o total da série vá além de qualquer número predeterminado, não importa quão grande. Diz-se que a série diverge para o infinito. Por outro lado, isso não acontece com séries de termos elevados ao quadrado

$$1 + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \frac{1}{5^2} + \frac{1}{6^2} + \dots$$

Estamos ainda usando o mesmo processo: somando números cada vez menores, mas dessa vez alcançamos um limite, e esse limite é menor do que 2. Drasticamente, a série converge para  $\pi^2/6 = 1,64493\dots$

Nessa última série a potência dos termos é 2. Na série harmônica a potência dos denominadores é silenciosamente igual a 1 e esse valor é crítico. Se a potência aumentar em uma quantidade minúscula para um número logo acima de 1 a série converge, mas se a potência diminui em uma quantidade minúscula para um valor logo abaixo de 1, a série diverge. A série harmônica fica no limite entre convergência e divergência.

**A função zeta de Riemann** A famosa função zeta de Riemann  $\zeta(s)$  na verdade já era conhecida por Euler no século XVIII, mas Bernhard Riemann reconheceu sua importância plena. A  $\zeta$  é a letra grega zeta, enquanto a função é escrita como:

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} + \dots$$

Foram calculados diversos valores da função zeta, mais notavelmente,  $\zeta(1) = \infty$  porque  $\zeta(1)$  é a série harmônica. O valor

de  $\zeta(2)$  é  $\pi/6$ , o resultado descoberto por Euler. Já foi mostrado que os valores todos de  $\zeta(s)$  envolvem  $\pi$  quando  $s$  é um número par enquanto a teoria de  $\zeta(s)$  para números ímpares de  $s$  é mais difícil. Roger Apéry provou o importante resultado de que  $\zeta(3)$  é um número irracional, mas esse método não se estendeu a  $\zeta(5)$ ,  $\zeta(7)$ ,  $\zeta(9)$ , e daí por diante.

**A hipótese de Riemann** A variável  $s$  na função zeta de Riemann representa uma variável real, mas pode ser estendida para representar um número complexo (ver p. 34). Isso permite que sejam aplicadas técnicas poderosas de análise complexa.

A função zeta de Riemann tem uma infinidade de zeros, ou seja, uma infinidade de valores de  $s$  para os quais  $\zeta(s) = 0$ . Em artigo apresentado na Academia de Ciências de Berlim em 1859, Riemann mostrou que todos os zeros importantes eram números complexos que jazem na faixa crítica limitada por  $x = 0$  e  $x = 1$ . Além disso, ele fez sua famosa hipótese:

*Todos os zeros da função zeta  $\zeta(s)$  de Riemann caem na linha  $x = 1/2$ , a linha ao longo do meio da faixa crítica.*

O primeiro passo real na direção de estabelecer essa hipótese foi tomado independentemente em 1896 por Charles de la Vallée-Poussin e Jackes Hadamard. Eles mostraram que os zeros devem ficar no interior da faixa (de modo que  $x$  não pode ser igual a 0 ou 1). Em 1914, o matemático inglês G.H. Hardy provou que uma infinidade de zeros fica ao longo da linha  $x = 1/2$ , embora isso não evite que haja uma infinidade de zeros fora dela.



No que diz respeito a resultados numéricos, os zeros não triviais calculados por volta de 1986 (1.500.000.000 deles) realmente situam-se na linha  $x = 1/2$ , enquanto cálculos atuais verificaram que isso é também verdadeiro para os primeiros 10 bilhões de zeros. Enquanto esses resultados experimentais sugerem que a conjectura é razoável, há ainda a possibilidade de que possa ser falsa. A conjectura é que todos os zeros se situam nessa linha crítica, mas isso ainda espera prova ou refutação.

**Qual a importância da hipótese de Riemann?** Há uma inesperada conexão entre a função zeta de Riemann  $\zeta(s)$  e a teoria dos números primos (ver p. 38). Os números primos são 2, 3, 5, 7, 11, e daí por diante, os números que só são divisíveis por 1 e por eles mesmos. Usando primos, podemos formar a expressão

$$\left(1 - \frac{1}{2^s}\right) \times \left(1 - \frac{1}{3^s}\right) \times \left(1 - \frac{1}{5^s}\right) \times \dots$$

e acaba que isso é um outro jeito de escrever  $\zeta(s)$ , a função zeta de Riemann. Isso nos diz que o conhecimento da função zeta de Riemann vai lançar luz sobre a distribuição dos números primos e enfatizar a nossa compreensão dos blocos de construção básicos da matemática.

Em 1900, David Hilbert estabeleceu seus famosos 23 problemas para matemáticos resolverem. Ele disse a respeito do oitavo problema, “se eu tivesse de acordar depois de ter dormido durante 500 anos, minha primeira pergunta seria: Já provaram a hipótese de Riemann?”

Hardy usou a hipótese de Riemann como um seguro ao cruzar o mar do Norte depois de sua visita de verão a seu amigo Harald Bohr, na Dinamarca. Antes de sair do porto, ele mandava a seu amigo um cartão postal com a reivindicação de que acabava de provar a hipótese de Riemann. Era um jeito inteligente de fazer duas apostas no mesmo cavalo. Se o barco naufragasse, ele teria a honra póstuma de ter resolvido o grande problema. Por outro lado, se Deus existisse, ele não deixaria que um ateu como Hardy tivesse essa honra e, portanto, evitaria que o barco afundasse.

A pessoa que rigorosamente resolver a questão vai ganhar um prêmio de 1 milhão de dólares, oferecidos pelo Clay Mathematics Institute. Mas dinheiro não é a força motriz – a maior parte dos matemáticos se contentaria em apenas alcançar o resultado e uma posição muito alta no panteão dos grandes matemáticos.

## **A ideia condensada: o supremo desafio**

# Glossário

**Álgebra** Trabalhando com letras em vez de números de modo a estender a aritmética, a álgebra é atualmente um método geral aplicável à matemática inteira e às suas aplicações. A palavra “álgebra” deriva de “*al-jabr*”, usada em um texto árabe do século IX d.C.

**Algoritmo** É uma receita matemática. Uma rotina estabelecida para resolver um problema.

**Axioma** Uma declaração para a qual não se busca nenhuma justificativa, usada para definir um sistema. O termo “postulado” serviu ao mesmo propósito para os gregos, mas para eles significava uma verdade autoevidente.

**Base** A base para um sistema numérico. Os babilônios baseavam seu sistema em 60, enquanto a base moderna é 10 (decimal).

**Cardinalidade** O número de objetos em um conjunto. A cardinalidade do conjunto  $\{a, b, c, d, e\}$  é 5, mas a cardinalidade pode também receber significado no caso de conjuntos infinitos.

**Comutativo** A multiplicação na álgebra é comutativa se  $a \times b = b \times a$ , como na aritmética comum (i.e.,  $2 \times 3 = 3 \times 2$ ). Em muitos ramos da álgebra moderna, esse não é o caso (p.ex., álgebra de matrizes).

**Conjunto** Uma coleção de objetos: por exemplo, o conjunto de alguns itens de mobiliário pode ser  $F = \{\text{cadeira, mesa, sofá, banco, armário}\}$ .



**Conjunto vazio** O conjunto sem objetos. Tradicionalmente representado por  $\emptyset$ , é um conceito útil na teoria dos conjuntos.

**Contraexemplo** O único exemplo que refuta uma declaração. Prova-se que a afirmação “todos os cisnes são brancos” é falsa com a presença de um único cisne negro como contraexemplo.

**Corolário** Uma consequência menor de um teorema.

**Correspondência um a um (biunívoca)** É a natureza do relacionamento quando cada objeto em um conjunto corresponde a exatamente um objeto em outro conjunto e vice-versa.

**Denominador** A parte de baixo de uma fração. Na fração  $3/7$ , o número 7 é o denominador.

**Diagrama de Argand** Um método visual para exibir o plano bidimensional dos números complexos.

**Diagrama de Venn** Um método pictórico (diagrama de balão) usado na teoria dos conjuntos.

**Diferenciação** Uma operação básica em Cálculo, que produz a derivada, ou a taxa de mudança. Para uma expressão que descreve como a distância depende do tempo, por exemplo, a derivada representa a velocidade. A derivada da expressão da velocidade representa a aceleração.

**Discreto** Termo usado em oposição a “contínuo”. Há intervalos entre valores discretos, como os intervalos entre os números inteiros 1, 2, 3, 4,...

**Distribuição** A gama de probabilidades de eventos que ocorrem

em uma experiência ou uma situação. Por exemplo, a distribuição de Poisson dá as probabilidades de  $x$  ocorrências de um evento raro acontecer para cada valor de  $x$ .

**Divisor** Um número inteiro que divide exatamente outro número inteiro. O número 2 é divisor de 6 porque  $6 \div 2 = 3$ . Do mesmo modo 3 é outro, porque  $6 \div 3 = 2$ .

**Eixos  $x$ - $y$**  A ideia devida a René Descartes de representar pontos graficamente com uma coordenada- $x$  (eixo horizontal) e coordenada- $y$  (eixo vertical).

**Expoente** Uma notação usada em aritmética. Ao se multiplicar um número por ele mesmo,  $5 \times 5$  é escrito como  $5^2$  com o expoente 2. A expressão  $5 \times 5 \times 5$  é escrita como  $5^3$ , e daí por diante. A notação pode ser ampliada: por exemplo, o número  $5^{1/2}$  significa a raiz quadrada de 5. Termos equivalentes são potência e índice.

**Expressão diofantina** Uma equação na qual as soluções têm de ser números inteiros, ou talvez, frações. Recebeu esse nome em honra ao matemático grego Diofanto de Alexandria (c.250 d.C.).

**Fração** Um número inteiro dividido por outro, por exemplo,  $3/7$ .

**Fração unitária** Frações com o numerador igual a 1. Os egípcios antigos basearam seu sistema numérico em parte em frações unitárias.

**Geometria** Ao tratar das propriedades de linhas, formas e espaços, o assunto foi formalizado nos *Elementos* de Euclides no século III a.C. A geometria permeia toda a matemática e atualmente perdeu seu significado histórico restrito.

**Hipótese** Uma afirmação preliminar à espera ou de prova ou de refutação. Tem o mesmo status matemático que a conjectura.

**Integração** É uma operação básica em Cálculo para medir área. Pode ser mostrada como sendo a operação inversa à diferenciação.

**Iteração** Começar com um valor  $a$  e repetir uma operação é chamado iteração. Por exemplo, começando com 3 e acrescentando repetidamente 5 vamos ter a sequência iterada 3, 8, 13, 18, 23,...

**Lema** É uma afirmação provada como uma ponte na direção da prova de um teorema maior.

**Matriz** Um conjunto de números ou símbolos arrumados em um quadrado ou retângulo. Os conjuntos podem ser acrescentados juntos e multiplicados, e podem formar um sistema algébrico.

**Máximo divisor comum, mdc** O mdc de dois números é o maior número que divide os dois exatamente. Por exemplo, 6 é mdc de 18 e 84.

**Numerador** A porção superior de uma fração. Na fração  $3/7$ , o número 3 é o numerador.

**Número primo** Um número inteiro que só tem como divisor 1 e ele mesmo. Por exemplo, 7 é um número primo, mas 6, não (porque  $6 \div 2 = 3$ ). Costuma-se começar a sequência de números primos com 2.

**Número quadrado** O resultado de multiplicar um número inteiro por ele mesmo. O número 9 é um número quadrado porque  $9 = 3$

× 3. Os números quadrados são 1, 4, 9, 16, 25, 36, 49, 64,...

**Números imaginários** São números que envolvem o “imaginário”  $i = \sqrt{-1}$ . Eles ajudam a formar os números complexos ao serem combinados com os números ordinários (ou “reais”).

**Números irracionais** São números que não podem ser expressos como uma fração (p.ex., raiz quadrada de 2).

**Números racionais** Números que são ou inteiros ou frações.

**Número transcendental** É um número que não pode ser solução para nenhuma equação algébrica, como  $ax^2 + bx + c = 0$ , ou onde  $x$  tem uma potência maior. O número  $\pi$  é um número transcendental.

**Poliedro** Uma forma de sólido com muitas faces. Por exemplo, um tetraedro tem quatro faces triangulares e um cubo tem seis faces quadradas.

**Primos gêmeos** Dois números primos separados por no máximo um número. Por exemplo, os gêmeos 11 e 13. Não se sabe se há uma infinidade desses gêmeos.

**Quadratura do círculo** O problema de construir um quadrado com a mesma área de um círculo dado usando-se apenas uma régua para traçar linhas retas e um par de compassos para traçar círculos. É impossível.

**Quaterniões** Números imaginários tetradimensionais descobertos por W.R. Hamilton.

**Raiz quadrada** O número que, quando multiplicado por ele

mesmo, é igual a um número dado. Por exemplo, 3 é a raiz quadrada de 9 porque  $3 \times 3 = 9$ .

**Resto** Se um número inteiro é dividido por outro número inteiro, o número que sobra é o resto. O número 17 dividido por 3 dá 5 com resto 2.

**Secções cônicas** O nome coletivo para a família clássica de curvas que inclui o círculo, linhas retas, elipses, parábolas e hipérbolas. Todas essas curvas são encontradas como secções transversais de um cone.

**Sequência** Uma linha (possivelmente infinita) de números ou símbolos.

**Série** Uma linha (possivelmente infinita) de números ou símbolos somados.

**Simetria** A regularidade de um formato. Se uma forma pode ser girada de modo a preencher sua impressão original, ela é dita como tendo simetria rotacional. Uma forma tem simetria especular se seu reflexo corresponde à impressão original.

**Sistema hexadecimal** Um sistema numérico de base 16, fundamentado em 16 símbolos, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E e F. É amplamente usado em computação.

**Sistema numérico binário** Um sistema numérico baseado em dois símbolos, 0 e 1, fundamental para cálculos computacionais.

**Sistema posicional** A magnitude de um número depende da posição de seus algarismos. Em 73, o valor de lugar do 7 significa “7 dezenas” e do 3 significa “3 unidades”.

**Solução ideal** Muitos problemas exigem a melhor solução, ou a ideal. Essa pode ser uma solução que minimize o custo ou maximize o lucro, como ocorre na programação linear.

**Teorema** É um termo reservado para um fato estabelecido de alguma importância.

**Teorema de Pitágoras** Se os lados de um triângulo retângulo tiverem os comprimentos  $x$ ,  $y$  e  $z$ , então  $x^2 + y^2 = z^2$ , onde  $z$  é o comprimento do lado maior (a hipotenusa) oposto ao ângulo reto.

**Teoria do caos** A teoria de sistemas dinâmicos que parecem aleatórios, mas têm uma regularidade subjacente.

# Índice

- Abel, Niels 60, 156
- álgebra 6, 9, 10, 58, 59, 60, 61, 62, 67, 68, 75, 100, 156, 158, 160, 161, 172, 206
  - curvas 92
  - e topologia 97
  - Fermat, último teorema de 198
  - genética 150
  - grupos abstratos 58, 61, 82, 153, 156, 201
  - matrizes 60, 158, 160, 161, 206
  - Pascal, triângulos de 55, 57
- algoritmos 62, 63, 64, 182, 185, 186, 189, 206
- ângulos
  - Euclides, postulados de 84
  - medidas 10, 88, 89, 94
  - triseção 82
- aniversário 137
- aniversário, problema do 134, 135, 136, 137
- apostas 127, 205
- área
  - círculo 23, 208
  - polígonos 23, 114
  - sob curva 81
  - triângulos 86, 87, 89
- Argand, diagrama de 34, 36, 206
- Aristóteles 30, 66, 67
- Arquimedes de Siracusa 22, 23, 25
- árvores 118, 121
- axiomas 61, 76, 77, 111, 129, 156, 157, 206
  
- base 4, 10, 11, 12, 13, 206
- Bayes, Thomas 130
- Benford, Frank 138, 139
- Bernoulli, Jacob 26, 91
- binário, sistema 13, 206
- borboleta, efeito 106, 109
- Bourbaki, Nicholas 74
- Brianchon, teorema de 117

caixeiro-viajante 186  
  problema do 186, 188, 189  
Cálculo 78, 81, 207  
Cantor, Georg 30, 31, 33, 74, 75, 77, 98  
caos, teoria do 106, 109, 206  
cardinalidade 31, 76, 77, 206  
catenária, curva 92  
Cayley, Arthur 100, 102, 104, 121, 123, 124, 154, 155, 158  
central, teorema do limite 142, 143, 144  
César, Júlio 162, 164  
chance 124, 126, 128, 129, 132, 133, 134, 136, 137, 139, 142, 144, 145, 163, 169  
círculo 22, 23, 37  
  pi ( $\pi$ ) 22, 23  
cobrir uma parede retangular  
  máximo divisor comum 63  
códigos 114, 162, 164  
coelho, problema do 52  
coincidência 135, 137, 175  
combinatória, análise 57, 166, 167, 169  
complexos, números 34, 35, 36, 37, 60, 103, 204, 206, 207  
compostos, juro 179, 181  
comutativo 206  
cônicas, secções 90, 94, 206  
conjuntos 30, 31, 69, 74, 75, 76, 77, 103, 207, 208  
  teoria dos 9, 69, 74, 76, 77, 207  
conjunto vazio 207  
construções 12, 46, 89, 154  
  proporção áurea 52  
contagem 18, 25, 30, 56, 118, 138, 166  
continuum, hipótese do 74, 77  
contraexemplo 67, 70, 71, 125, 206  
cor  
  genética 101, 150, 153  
  problema das quatro cores 4, 122, 123, 124  
cordas, teoria das 98, 99, 101  
corolário 206  
correlação 146, 147  
correspondência um a um (biunívoca) 31, 32, 208  
criptografia 62, 162, 164  
cubo, números ao 41, 59, 198



- curvas 29, 90, 92
  - algébricas 92
  - cálculo 81
  - clássicas 90, 92
  - Koch, floco de neve 104, 105
  - normal 142, 144, 145
  - teoria das 201
- da Vinci, Leonardo 52, 53, 91, 98
- decimais, números 12, 13
  - conversão de frações 16
- decimal
  - origens 10
- deficientes, números 42, 43
- De Morgan, Augustus 69, 70, 72, 75, 122, 123
- denominador 8, 14, 15, 16, 206
- Descartes, René 34, 44, 45, 70, 91, 92, 209
- detecção de erros, códigos 162, 163, 164
- dieta, problema da 182, 184
- diferenciação 78, 81, 206
- dimensão fracionária 102, 105
- dimensões 32, 37, 50, 60, 94, 97, 98, 99, 100, 101, 155, 173, 200
  - fracionárias 101, 105
- diofantinas, equações 64, 198, 199, 206
- direto, método 70, 71
- discreta, geometria 114, 116, 117, 169
- discreto 206
- distribuições 138, 141, 142, 143, 144, 145, 152, 153, 202, 205, 207
- divisão
  - Algoritmo de Euclides 63
  - zero 7, 8
- divisor 207
- DNA 91, 150, 153
- dodecaedro 95
- Dudeney, Henry 178, 181
- Dürer, Albrecht 171, 172
- e 26, 28, 29
- egípcios 10, 14, 17, 209
- Einstein, Albert 77, 79, 99, 110, 113, 115, 134, 137, 179, 194, 196, 197
- elipse 91, 117

equações 34, 58, 59, 60, 64, 92, 100, 109, 182, 195, 196, 197, 198

quadráticas 28, 60

esferas 97, 100, 113

espaço-tempo 99, 101, 113, 197

espiral logarítmica 91

estatística

conexão de dados 146

curva normal 142

probabilidade 130

Euclides de Alexandria 31, 98

algoritmo 62, 63, 64

construção de polígonos 84, 85

CQD 72

Elementos 110

números perfeitos 42, 45

números primos 38, 40

postulados de 77, 110, 111

triângulos 86, 87

Euler, Leonhard 5

e 28

e 26

Euler, fórmula de 94, 95

Euler, linha de 87, 88

Fermat, último teorema de 200

gráficos 118

números perfeitos 45

pi ( $\pi$ ) 23, 24

quadrado latino 174, 175, 176, 177

quadrados elevados ao quadrado 170, 172

teorema de 119, 162, 165

expoente 207

Fano, plano de 114, 116, 117

fatoriais, números 167, 168

Fermat, Pierre de 198

números primos 41, 85

probabilidade 127

último teorema de Fermat 4, 172, 198, 201, 202

Fibonacci, sequência de 46, 48, 49, 52

financeira, matemática 178

dieta, problema da 182

juros 178  
fração unitária 209  
frações 10, 11, 14, 15, 16, 17, 21, 27, 32, 207, 209  
  contagem 32  
  conversão para decimais 16  
  conversão pra decimais 16  
  raiz quadrada 20  
  Riemann, hipótese 202  
fractais 101, 102, 103, 104, 105  
Franklin, Benjamin 171, 172  
fuzzy, lógica 69

Galileu 80, 194, 195  
Galton, Francis 123, 146, 148  
Gauss, Carl Friedrich 22, 34, 39, 41, 82, 85, 112, 113, 142, 146, 182  
Gelfond, constante de 28  
genética 150, 151, 153  
geometria 207  
  dimensão 99  
  discreta 114, 116, 117, 169  
  elíptica 113  
  euclidiana 101, 110, 113, 116  
  hiperbólica 112, 113  
  paralelas, postulado das 110  
  projetiva 114, 116  
  topologia 94  
Gödel, teorema de 76  
Goldbach, conjectura de 38, 40  
gráficos 109, 118, 120  
grafos não planares 120  
Grassmann, Hermann 61, 100  
gravidade 8, 79, 197  
grupos, teoria dos 154, 169

Halmos, Paul 72, 125  
Hamilton, sir William Rowan 34, 37, 60, 61, 208  
Hardy, G.H. 55, 150, 151, 152, 153, 170, 202, 204, 205  
Heawood, Percy 122, 123, 124  
hexadecimal, sistema 13, 207  
hieróglifos 17, 167  
Hilbert, David 77, 101, 202, 205

hipérbole 90, 117, 206

hiperespaço 99, 100

hipótese 207

i 29, 34, 35, 37, 179, 181

icosaedro 95

ideal, solução 208

imaginários, números 34, 35, 41, 172, 207, 208

indireto, método 72, 73

indo-arábicos, números 6, 10

indução matemática 70, 72, 73

infinito ( $\infty$ ) 8, 30

integração 78, 81, 207

irracionais, números 18, 21, 32, 84, 207

iteração 103, 207

jogos, teoria dos 4, 190, 191

Jordan, Camille 92, 93

juros 26, 27, 178, 179, 180, 181

Kirkman, rev. Thomas 114, 117, 166, 169

Klein, garrafa de 97

Koch, floco de neve 102, 104, 105

Lagrange, Joseph 41, 156

Laplace, marquês Pierre-Simon-de 106, 107, 126, 142

latinos, quadrados 169, 174, 175, 176, 177

Legendre, Adrien Marie 111, 146, 198, 200

Leibniz, Gottfried 57, 78, 80, 81

lema 207

lemniscata 92

Leonardo de Pisa (Fibonacci) 7, 14, 46, 50

limaçon 92

lineares, equações 58, 59, 109

linear, programação 182, 184, 185, 208

logarítmica, espiral 91

logaritmo 20, 26, 84

lógica 21, 60, 66, 67, 68, 69, 70, 73, 78, 84, 190

Lo Shu, quadrado 170, 171

luz, velocidade da 194, 195, 196, 197

Mandelbrot, conjunto de 102, 103

manifolds 97  
mapas, quatro cores 125  
matrizes 158, 159, 160, 161, 207  
máximo divisor comum (mdc) 63, 64, 65, 207  
máximo fator comum 63  
médias 144  
Mendel, Gregor 150, 153  
Mersenne, números de 40, 42, 44, 45  
minimax, teorema 193  
mínimo múltiplo comum (mmc) 63, 64  
mnemônico, pi 25  
Möbius, fita de 94, 96  
Morse, código 162, 164  
movimento 74, 79, 91, 92, 107, 108, 194, 197  
movimento de três barras 92  
multiplicação 12  
    cruzada 7, 8  
    frações 15, 16, 17  
    matrizes 159, 160  
    números imaginários 35, 36  
    zero 7, 8  
  
Napoleão, teorema de 88  
Nash, John F. 190, 191  
Navier–Stokes, equações de 109  
Newton, Isaac 22, 78, 79, 80, 90, 92, 99, 113, 194, 195, 197  
normal, curva 142, 144, 145  
notação científica 13  
numerador 9, 14, 15, 208  
numerologia 41, 44  
números amigáveis 42, 44  
números negativos 34, 35  
números perfeitos 42, 43, 44, 45  
números quadrados 18, 19, 198, 208  
números racionais 15, 208  
números reais 32, 33, 34, 35, 36, 37, 74, 77, 103, 114  
  
octaedro 95  
  
papel, tamanhos 50  
parábola 19, 90, 91, 92, 93, 117

paralelas, linhas 110, 113, 116  
paralelas, postulado das 110  
Pascal, Blaise  
    Pascal, teorema de 114, 117  
    Pascal, triângulos de 54, 55, 56, 57  
    probabilidade 126, 134  
Pearson, correlação de 146, 147  
pêndulos 107, 108, 109  
pi ao quadrado 203  
Pick, teorema de 115  
Pitágoras 18, 87, 91  
    teorema de 20, 52, 86, 87, 199, 201, 208  
pi ( $\pi$ ) 20, 22, 23, 24, 25, 26, 27, 28, 32, 34, 35, 49, 84, 204, 209  
Poincaré, Henri 97, 104, 106  
    Poincaré, conjectura de 94, 97, 202  
Poisson, distribuição de 29, 138, 139, 207  
poliedros 94, 95, 96, 208  
polígonos 82, 84, 85  
polinomial, tempo 189  
ponte treliçada (Warren treliça) 89  
posicional, sistema 208  
previsão do tempo 109, 133  
previsões 141  
primos gêmeos 40, 209  
    problema dos 40  
primos, números 38, 39, 40, 41, 42, 43, 49, 65, 85, 165, 173, 202, 205, 208, 209  
prisioneiro, dilema do 190, 193  
probabilidade 29, 78, 126, 127, 128, 129, 130  
    Bayes, fórmula de 130, 131, 132, 133  
    condicional 130, 131  
    distribuição 29, 144, 145, 152  
    e 29  
    genética 151, 152, 153  
    inversa 130  
    normal, curva 142, 144, 145  
    problema do aniversário 135, 136, 137  
    teoria da 129  
proporção áurea 51  
prova 21, 40, 70, 71, 72, 73, 84, 87, 125, 132  
quadrados

- latinos 174, 175, 176, 177
- mágicos 4, 170, 171, 172, 173, 175
- quadrados mágicos 4, 170, 171, 172, 173, 175
- quadratura do círculo 24, 82, 83, 84, 208
- quaterniões 60, 61, 172, 208
  
- raciocínio 66
- racionais, números 208
- raiz quadrada 19, 20, 21, 24, 72, 199, 207, 208
  - de  $-1$  34, 35
- razão áurea 52
- regressão 146, 148, 149
- relatividade 77, 110, 113, 194, 196, 197
- resto 16, 208
- retângulos áureos 4, 50, 51, 52, 53
- Riemann, Bernhard 78, 110, 113, 202, 204
  - geometria elíptica 113
  - Riemann, hipótese de 4, 202, 204, 205
- romanos, algarismos 11
- rosca 94, 96, 124
- Russell, Bertrand 75
  
- sequência 208
- séries 208
- Sierpiński, gaxeta de 56, 104
- silogismo 66, 67
- simetria 54, 55, 57, 100, 126, 154, 155, 156, 208
- simetria especular 55, 56, 154, 155, 209
- simetria rotacional 154, 155, 209
- sistemas numéricos 10, 11
- Sistema Triplo de Steiner (STS) 117
- soma
  - frações 202
  - matrizes 159
  - números imaginários 34, 35
  - zero 6, 7
- Spearman, correlação de 147, 148
- Stokes, George Gabriel 109
- subtração
  - zero 7
- Sudoku 4, 169, 174

superabundantes, números 42, 43  
superáurea, proporção 49  
superáureo, retângulo 53

teorema 70, 71, 209  
teorema chinês do resto 62, 65  
teorema do aperto de mão 119, 120  
tetraedro 55, 95  
topologia 90, 93, 94, 96, 97, 101  
torus 124

transcendental, número 209

transporte 185

triangulares, números 18, 19, 55

triângulos 20, 23, 86, 87

    construção 83, 84, 85

    de Leibniz 57

    de Pascal 54, 55

    Fano, plano de 116

    geometria elíptica 113

    Sierpiński, gaxeta de 104

    simetria 155, 156

trigonometria 86, 88, 89

tripé 154, 156, 157

tríscele 154, 155, 156

unidade 37

valor de lugar, sistema 10, 208

Venn, diagrama de 74, 209

viagem 161

Von Lindemann, Ferdinand 24, 28, 84, 198, 201

Von Neumann, John 190, 191

Weinberg, Wilhelm 150, 151

Wiles, Andrew 198, 201

x-y, eixos 93, 209

Zermelo-Fraenkel, axiomas 76, 77

zero 6, 7, 8, 9, 12, 13, 204

zeta, função 204, 205



1 Numa meia-noite agreste, quando eu lia, lento e triste, / Vagos, curiosos tomos de  
ciências ancestrais, (Tradução de Fernando Pessoa)

1 Com muitos fatos jubilosos a respeito do quadrado da hipotenusa. Sou muito bom em cálculo integral e diferencial.

1 Eu ia para St. Ives,/ Encontrei um homem com sete esposas;/ Cada esposa tinha sete sacos,/ Cada saco tinha sete gatos,/ Cada gato tinha sete gatinhos/ Gatinhos, gatos, sacos e esposas,/ Quantos iam para St. Ives?