Unidade 10

Números e Codificação de Mensagens

Agora trataremos de assuntos atuais:
computadores, informação e códigos.

Criptografia é um assunto em que ocorre uma feliz confluência do passado e do presente, dos aspectos puro e aplicado da Matemática. É um bom exemplo de por que as questões matemáticas são importantes e continuam a atrair o interesse e a energia de tantas pessoas.

Texto 35: A Matemática às Portas de um Novo Milênio

Terminamos a unidade didática anterior mencionando Hilbert e sua lista de 23 problemas, que ele acreditava guiariam o desenvolvimento da Matemática no século 20.

Você deve estar se perguntando: o que aconteceu com a Matemática no século que findou? Teria algum matemático tão famoso quanto Hilbert elaborado uma lista de questões visando o século 21?

Isso sem contar que inauguramos, também, um novo milênio.

Pois bem, quanto à primeira pergunta, podemos dizer que a Matemática superou as mais audazes expectativas. Em termos de volume de produção, diversificação, criação de novas áreas de interesse e atividades interdisciplinares, o crescimento tem sido exponencial.

A atividade de pesquisa continuou fortíssima por todo o século 20, mesmo nos momentos mais difíceis pelos quais a humanidade passou.

A comunidade matemática manteve-se em contato, trocando informações sobre

a maioria dos tópicos de pesquisa, até durante os períodos mais duros.

Por exemplo, enquanto americanos e os, então, soviéticos se engalfinhavam na chamada corrida pelo espaço, matemáticos desses países mantinham suas relações em bons termos.

É tradição na Matemática que toda informação nova seja disponibilizada permitindo que matemáticos de diferentes partes do mundo desenvolvam seus potenciais completamente.

Teorema das Quatro Cores

Quatro cores são suficientes para colorir qualquer mapa plano, dividido em regiões, de tal forma que regiões vizinhas não partilhem a mesma cor. Regiões que só se tocam num ponto não são consideradas vizinhas.

Uma coisa que marcou definitivamente a atividade matemática no século 20 foi o advento dos computadores, como o fez em todos os outros setores da atividade humana. Isso ocorreu diretamente, em certos casos. Um exemplo famoso é a demonstração do Teorema das Quatro Cores, que só pode ser completada com a ajuda deles.

Os computadores ampliaram imensamente nossa percepção matemática. Ganhamos amplos poderes computacionais, antes restritos a poucas e privilegiadas pessoas, como Euler e Gauss, além de uma melhor visualização de objetos matemáticos. É claro que isso é apenas a ponta de um iceberg.

Também cumprem importante papel na comunicação. Grupos de pesquisas espalhados pelo mundo mantêm-se em contato, trocando informações o tempo todo. Isso é reflexo de uma outra característica marcante da Matemática nos nossos dias: ela tornou-se uma atividade bastante gregária.

Aqui entra o tema dessa unidade: a criptografia. Mais do que nunca, em nossos dias a informação tornou-se um bem valiosíssimo. Trocar e acumular dados de modo seguro é, a um só tempo, tarefa difícil e relevante.

Mas, antes de falarmos sobre esse assunto e sobre os temas de Matemática que estão a ele relacionados, você precisa saber se há uma nova lista de problemas para o próximo século. Afinal de contas, há uma pergunta a ser respondida.

35.1 O Ano Mundial da Matemática

A União Matemática Internacional, em congresso realizado em 6 de maio de 1992, no Rio de Janeiro, propôs o ano 2000 como o Ano Mundial da Matemática

e definiu três objetivos para o 2000AMM:

- indicação dos grandes desafios da Matemática para o século 21;
- promulgação da Matemática, pura e aplicada, como uma das principais chaves para o desenvolvimento;
- reconhecimento da presença constante da Matemática na sociedade de informação.

No lugar de uma lista com problemas, o encontro produziu o livro *Mathematics: Frontiers and Perspectives (Matemática: Fronteiras e Perspectivas)*, editado por quatro expoentes da Matemática: Vladimir Arnold, Michael Atiyah, Peter Lax e Barry Mazur. Trata-se de uma coletânea de artigos em que matemáticos de uma grande variedade de áreas contribuem com suas impressões e expectativas.

Um olhar sobre os colaboradores para a coletânea deixa a certeza de que a Matemática continuará a brilhar por todo o século e, depois, também. Além dos quatro editores, cooperaram para o livro nomes como Steve Smale e Peter Lax. Smale é americano, ganhador da Medalha Fields de 1966, e escreveu o artigo *Mathematical problems for the next century (Problemas matemáticos para o próximo século)*, que contém uma lista de 18 problemas. Lax foi diretor do Courant Institute, em New York, e tem interesse em Matemática e Computação, como podemos ver no título de sua contribuição: *Mathematics and computing (Matemática e computação)*.

Apesar de sujeito a críticas, o livro é uma prova da diversidade e vigor da atividade matemática.

Agora, enfocaremos especificamente criptografia.

Texto 36: Criptografia

O objetivo da criptografia é obter métodos de codificar uma mensagem de modo que apenas seu destinatário possa interpretá-la.

A palavra *criptografia* tem origem (surpresa!) grega. *Cryptos* significa secreto, oculto.

Do ponto de vista matemático, queremos um *isomorfismo*, uma maneira de *transformar* uma mensagem que se pretende transmitir em algo ilegível, mas

que, ao chegar ao destinatário, este possa transformá-la de volta, na mensagem original. Chamamos *cifrar* o processo de transformar a mensagem original em um texto ilegível e *decodificar* o processo reverso. Reservamos a palavra *decifrar* para significar a descoberta do processo todo. Isto é, estamos fazendo uma distinção quanto à ação de *decodificar* uma mensagem cifrada por um método criptográfico, sem descobrir como ele funciona globalmente, da ação de *decifrar* o método, completamente.

Um exemplo simples de código consiste em permutar cada letra do alfabeto usada na mensagem pela letra seguinte. Por exemplo, a frase "A vida é bela" seria escrita codificada como "BWJEBFCFMB". O processo reverso daria "AVIDAEBELA". Esse método é bastante simples e fácil de ser *decifrado*. Note, por exemplo, que a mensagem cifrada começa com a letra B, que se repete mais duas vezes, enquanto que F aparece, ao todo, duas vezes. É conhecido que A é a letra mais usada em português, o que nos faz crer que B é o codificado de A.

36.1 A Cifra de Vigenère

Em 1586, o francês Blaise Vigenère publicou um livro contendo um método de cifrar mensagens que ficou conhecido pelo nome *cifra de Vigenère*.

Blaise Vigenère (1523 - 1596) Em função de sua atividade diplomática, começou a se interessar por criptografia e propôs a tabela no livro *Traité des chiffres ou secrètes manières d'écrire (Tratado das cifras ou modos secretos de escrever).*

O progresso feito em relação aos métodos anteriores consiste no fato de a maneira de permutar as letras para gerar a mensagem cifrada varia de letra para a letra.

A variação depende de uma palavra (ou frase) *chave* e há uma tabela conhecida de todos que codificam segundo o método. No início do processo o codificador escolhe uma palavra chave e a usa na codificação. Para que a mensagem seja decodificada, o destinatário precisa da palavra chave.

Para dar um exemplo, precisamos da tabela. (Veja adiante.) Para codificar a frase "A vida é bela" usaremos a palavra chave "Roma".

O processo consiste em colocar sobre a mensagem a ser cifrada a palavra chave, repetindo-a sucessivamente, de modo que a cada letra da mensagem corresponda uma letra da chave. Observe o exemplo:

R O M A R O M A R O
A V I D A E B E L A

Para codificar a letra A, usamos a linha 17 da tabela correspondente à letra R. A letra A se encontra na coluna 1. Portanto, A será codificado como R. Verifique na coluna 1 da linha 17, na tabela.

Para codificar a letra V usamos a linha 14, relativa à letra O. A letra V está na coluna 22, corresponde à letra J. Veja na coluna 22 da linha 14, na tabela.

Prosseguindo assim, obtemos a mensagem cifrada: RJUDRSNECO.

Para decodificar a mensagem, dispomos a palavra chave sobre a mensagem cifrada e executamos o processo reverso.

R	O	M	A	R	O	M	A	R	O
R	J	U	D	R	S	N	E	C	O

Veja, a letra S, da mensagem cifrada, aparece sob a letra O. A linha correspondente ao O é a 14, na qual o S se encontra na coluna 5. Na tabela, a coluna 5 tem ao alto a letra E, que aparece acentuada na frase: "A vida é bela."

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Charles Babbage (1791 - 1891) Projetou a *Máquina das Diferenças* e a *Máquina Analítica*. Eram calculadoras sofisticadas, precursoras do computador.

Friedrich Wilhelm Kasiski nasceu em novembro de 1805 numa pequena cidade da Prússia ocidental. Seu interesse por criptologia começou durante a carreira militar. Publicou "Die Geheimschriften und die Dechiffrierkunst" (As escritas secretas e a arte da decifração) em 1863.

Uma inconveniência desse código é o fato de que a mensagem, assim como a chave, devem chegar ao destinatário. Isto é, a Cifra de Vigenère é um exemplo de criptografia de chave simétrica. Apesar dessa característica, ela foi usada por muito tempo.

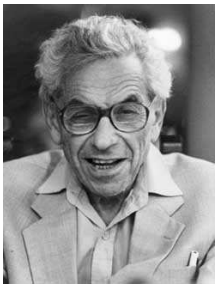
Por volta de 1855, um inglês chamado Charles Babbage descobriu como *quebrar* o código de Vigenère. Babbage foi um gênio, porém um tanto excêntrico. Ele também divisou a construção de um computador, em pleno século 19, contudo, não chegou a realizá-la. Babbage não divulgou sua descoberta de como decifrar o código de Vigenère e, em 1863, o criptógrafo Friedrich Wilhelm Kasiski, oficial da reserva do exército prussiano, publicou um método que permitia quebrar o código de Vigenère. O princípio desse método consiste em descobrir a palavra chave, começando por determinar seu comprimento.

Que tal uma interrupção na leitura? Aqui está uma oportunidade para você experimentar como funciona a decodificação do código de Vigenère.

Atividade 39

Decodifique a mensagem

QZQVSQVQHWIJWOSFVUHS



Paul Erdös (1913 - 1996) não tinha posição alguma em universidades ou institutos de pesquisa e passou a vida viajando, visitando amigos matemáticos com quem trabalhava.

usando o código de Vigenère e a palavra chave ERDOS.

O húngaro Paul Erdös foi um dos mais singulares e brilhantes matemáticos do século 20.

Seu principal interesse era a Teoria de Números e a frase que você decifrou na atividade anterior, usando o nome dele como chave, era a saudação que ele usava ao chegar para visitar algum de seus muitos colaboradores de pesquisa.

Ele costumava dizer que "um matemático é uma máquina de transformar café em teoremas".

Veja, agora, como foi importante o papel de outro matemático na decifração de um verdadeiro enigma.

Decifrando a *Enigma*

Você deve estar se perguntando se haveria algum erro no título dessa seção. Bem, a resposta é não. A Enigma era uma máquina de codificar. Depois das descobertas de Kasiski e Babbage, os criptógrafos necessitavam de novas cifras. Assim, foram inventadas máquinas criadoras de códigos que desempenharam um papel importante, especialmente durante os vários conflitos vividos pela humanidade na primeira metade do século 20.

Durante a Segunda Guerra Mundial, os alemães desenvolveram uma máquina de codificar que ficou conhecida por Enigma. Quebrar o código da Enigma passou a ser uma questão literalmente de vida ou morte. Um matemático inglês desempenhou, nesse episódio, papel fundamental. Ele se chamava Alan Turing.

Alan Turing (1912 - 1954) Era professor no King's College, Cambridge e trabalhava com teoria de máquinas, em projetos que anteciparam os modernos computadores.

Turing foi convocado pelo governo britânico e trabalhou na quebra do código aparentemente inviolável gerado pela Enigma. Os esforços de mais de sete mil funcionários, somados com as descobertas feitas por um criptólogo polonês, Marian Rejewski, de como funcionava uma versão primitiva da Enigma, e mais a perspicácia de Turing permitiram uma proeza fenomenal que deu aos aliados uma vantagem sem igual na virada do conflito.

É pena que Alan Turing não tenha recebido em vida as devidas homenagens. Primeiro, devido à natureza sigilosa da atividade, os trabalhos desse time de decifradores permaneceu em segredo por décadas. Mas é triste saber que Turing sofreu por intolerância e preconceito da sociedade em que viveu, por ser homossexual declarado. As pressões e humilhações foram tantas que ele, deprimido, cometeu suicídio.

O papel da Matemática na produção de novas cifras e na atividade de quebrá-las passou a ser cada vez mais importante.

Teoria de Números desempenha papel crucial num dos códigos mais usados na transmissão de dados por computadores, chamado RSA.

Texto 37: Números Primos, de Novo...

As questões típicas de Teoria de Números sempre exerceram um grande fascínio sobre matemáticos amadores e profissionais, seja pela simplicidade de suas for-

mulações, seja pela dificuldade que geralmente carregam.

Vamos passar rapidamente em revista alguns principais tópicos desse assunto.

Os gregos, em particular os pitagóricos, estudaram os números extensivamente e perceberam a importância dos números primos. Eles tinham um profundo interesse pelos números perfeitos e pelos pares de números amigáveis.

Nos Elementos de Euclides encontramos a prova de que há uma infinidade de primos, a primeira demonstração por absurdo de que temos notícia e, ainda, que todo número da forma $2^{n-1}(2^n-1)$, com 2^n-1 primo, é perfeito.

Posteriormente, Eratóstenes descobriu como determinar todos os números primos menores do que um certo número dado, usando o *crivo de Eratóstenes*. Aqui estão os primos menores do que 49.

~~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~~

Novos progressos só ocorreram com os trabalhos de Fermat, no início do século 17. Fermat conhecia algum *método de fatoração*, pois foi capaz de fatorar $2027651281 = 44021 \times 46061$ em relativamente pouco tempo.

Outra grande contribuição sua foi o Pequeno Teorema de Fermat.

37.1 Testes de primalidade

Uma questão de relevo a respeito de números inteiros é decidir se um dado número é primo ou não. Caso o número seja decomponível, a questão seguinte é descobrir sua fatoração, algo substancialmente mais difícil.

O resultado de Fermat é importante porque dá um critério de primalidade.

Como exemplo da dificuldade dessa questão, examinemos os números $M_n = 2^n - 1$, conhecidos como números de Mersenne. Uma condição necessária para que M_n seja primo é que n seja primo. No entanto, $M_{11} = 2047 = 23 \times 89$ é um número composto, apesar de 11 ser primo.

O maior número primo conhecido (em fevereiro de 2005) é o quadragésimo segundo número de Mersenne primo, $M_{25\,964\,951}$, que tem $7\,816\,230$ dígitos.

Neste ponto da história, entra em cena um de nossos campeões – Leonhard Euler.

A abordagem usada por Euler para mostrar que $2^{32}+1$ é um número composto é uma prova de que temos muito o que aprender com as idéias dos mestres do passado.

Veja qual foi a estratégia por ele usada.

37.2 Euler e os números primos

Fermat acreditava que os números da forma $2^{2^n}+1$ seriam primos. Isso é verdade para $n=1,2,3$ e 4, onde temos $2^{2^n}+1=5$, 17, 257 e $65\,537$, respectivamente, todos primos. Porém, $2^{32}+1$ é um pequeno gigante $4\,294\,967\,297$.

Como você já sabe, Euler demonstrou vários resultados enunciados por Fermat, inclusive o seu Pequeno Teorema. Note que Euler usou esse resultado para provar que $2^{32}+1$ é composto, contrariando a hipótese de Fermat.

Euler começou observando o seguinte:

> Se a é um número par e p é um primo que não é um fator de a mas divide a^2+1, então $p=4k+1$, para algum inteiro k.

Por exemplo, seja $a=8$. Então, $8^2+1=65=5\times 13$, tem fatores primos 5 e 13. Em ambos os casos, p é da forma $4k+1$.

Veja, a seguir, como Euler mostrou, usando o Pequeno Teorema de Fermat, a afirmação acima.

O fato de p dividir a^2+1, um número ímpar, indica que p é ímpar. Agora, todo número ímpar é da forma $4k+3$ ou $4k+1$. Portanto, para provar o resultado, bastava mostrar que a possibilidade $p=4k+3$ não ocorre.

A demonstração será por absurdo. Suponhamos que $p=4k+3$. Como p é primo, o Pequeno Teorema de Fermat garante que p divide $a^p-a=a\,(a^{p-1}-1)$. Por hipótese, p não é um fator de a. Concluímos que p divide $a^{p-1}-1$.

Assim, p divide $a^{p-1}-1 \;=\; a^{4k+2}-1$. Usaremos essa informação em breve.

Por outro lado, a fatoração

$$(a^2+1)\,(a^{4k}-a^{4k-2}+a^{4k-4}-\cdots+a^4-a^2+1) \;=\; a^{4k+2}+1,$$

e o fato de que p divide, por hipótese, a^2+1, garante que p divide $a^{4k+2}+1$.

Reunimos, agora, essa informação com a anterior:

Como p divide $a^{4k+2}-1$ e $a^{4k+2}+1$, também divide a diferença, ou seja:

$$p \text{ divide } (a^{4k+2}+1)-(a^{4k+2}-1) \;=\; 2.$$

Mas isso é uma contradição, pois p é ímpar por hipótese.

Logo, p é da forma $4k+1$, para algum k, como foi enunciado.

Para que você ganhe um pouco mais de percepção desse fato, tente fazer a atividade a seguir.

Atividade 40

Determine os fatores primos de 8^4+1 e mostre que eles são da forma $8k+1$.

Agora, vamos continuar com Euler que, prosseguindo, provou uma seqüência de resultados que culminou em:

Se a é par, p é primo e p divide $a^{32}+1$, então p é da forma $64k+1$.

Armado dessa informação, ele atacou a questão de fatorar $2^{32}+1$. Os resultados obtidos indicavam *bons* candidatos à fatoração. Quais são os primos da forma $64k+1$? Isso ocorre para os casos de $k=3$, 4, 7, 9 e 10, por exemplo, onde $p=193$, 257, 449, 577 e 641, respectivamente.

Uma das grandes contribuições de Euler para a Teoria de Números foi perceber que certas técnicas de análise matemática poderiam ser usadas no estudo dos números.

Os quatro primeiros primos não dividem $2^{32}+1$. Mas quando Euler fez a conta com 641, obteve a recompensa pelo trabalho: $2^{32}+1 = 4\,294\,967\,297 = 641\times 6\,700\,417$.

37.3 Outras contribuições para a Teoria de Números

Se nos surpreendemos com o fato de que a série harmônica $\sum_{n=1}^{\infty}\frac{1}{n}$ diverge, surpresa ainda maior vem do fato de que a soma dos inversos dos números primos

$$\frac{1}{2}+\frac{1}{3}+\frac{1}{5}+\frac{1}{7}+\frac{1}{11}+\frac{1}{13}+\ldots$$

também diverge.

Uma das questões que interessou as gerações de matemáticos após Euler foi a distribuição dos primos. Por exemplo, Dirichlet demonstrou em 1837 o seguinte teorema, conjecturado por Gauss:

> Se $(a, b) = 1$ (a e b são relativamente primos), então a progressão aritmética $a+b, 2a+b, 3a+b, \ldots$ contém uma infinidade de números primos.

Esse resultado generaliza o teorema da infinitude de primos.

Veja algumas questões abertas a respeito de números primos:

- há uma infinidade de números primos da forma $n^2 + 1$?
- sempre há um primo entre n^2 e $(n + 1)^2$?
- a seqüência de Fibonacci contém um número infinito de números primos?
- há uma infinidade de primos gêmeos (como 11 e 13, 41 e 43)?

A falta de um padrão aparente de distribuição dos números primos entre os números inteiros indica a riqueza do tema. Gauss e Legendre foram pioneiros ao tratarem desse assunto.

Chamamos de $\pi(n)$ o número de primos menores ou iguais a n.

Por exemplo, $\pi(10) = 4$, $\pi(20) = 8$, $\pi(50) = 15$.

Legendre conjecturou que

$$\pi(n) \sim \frac{n}{\ln(n) - 1.0836},$$

dando uma estimativa para $\pi(n)$. O número 1.0836 é chamado de constante de Legendre.

Gauss, por sua vez, acreditava que

$$\pi(n) \sim \mathrm{Li}(n) = \int_2^n \frac{1}{\ln x}\, dx.$$

É admirável o esforço que Gauss e Legendre despenderam. Devemos lembrar que eles não dispunham de computadores ou sequer uma simples máquina de calcular.

Estima-se que Gauss tenha contado todos os primos até três milhões. Ou seja, que ele tenha calculado $\pi(3\,000\,000)$.

O $216\,816$-ésimo primo é o número $2\,999\,999$ e o seguinte é $3\,000\,017$.

O que ficou conhecido como *Teorema dos Números Primos* é

$$\lim_{n\to\infty} \frac{\pi(n)}{n/\ln(n)} = 1.$$

Uma área que desperta muito interesse atualmente consiste em encontrar formas de determinar se um dado número é primo. Há dois tipos de testes, basicamente:

- testes probabilísticos – em que se usam computadores;
- testes de natureza teórica – como o teste de Lucas-Lehmer.

Pode-se dizer que há grande demanda por números primos.

O Teorema dos Números Primos foi demonstrado em 1896 pelo matemático francês Jacques Hadamard (1865 - 1963) e, independentemente, por Charles Jean Gustave de la Vallée Poussin (1866 - 1962), matemático belga. Parece que Teoria de Números é uma espécie de elixir da longa vida.

Veja, agora, como os números primos exercem papel importante na criptografia RSA.

Texto 38: Criptografia RSA

A sigla RSA provém dos sobrenomes de Ronald L. Rivest, Adi Shamir e Leonard Adleman, que trabalhavam no MIT (Massachusetts Institute of Technology) quando inventaram esse código, em 1978.

RSA é um exemplo de criptografia de chave assimétrica. Isto é, há uma chave pública, que todos podem conhecer, que serve para cifrar a mensagem. Porém, há uma chave privada, que é usada para decodificar a mensagem.

Veja como funciona, em linhas gerais: para cifrar uma mensagem utiliza-se um número $n = p\,q$, produto de dois primos. Essa é a chave pública.

A chave privada consiste dos dois fatores primos de n: p e q. Para decodificar a mensagem não basta conhecer n, é necessário usar seus fatores primos. Parece estranho, não? Conhecendo n, sabemos, *teoricamente*, seus fatores primos. No entanto, o funcionamento do método se baseia no fato de que, para números grandes (mais de 150 algarismos), com os métodos atuais, é impossível determinar p e q. Não é irônico que um método deposite toda a sua eficiência na incapacidade de se fazer alguma coisa teoricamente possível?

Há muita literatura disponível sobre esse fascinante aspecto da Matemática atual.

Assim chegamos ao fim de nossa disciplina, mas não ao fim da história.

Esperamos que no decorrer desse tempo que passamos juntos você tenha percebido a importância das questões matemáticas.

Lembre-se, as questões podem ser antigas, mas as idéias são atemporais.

Concluímos com uma frase memorável de Godfrey Harold Hardy, um matemático do século 20, que, ao lado de John Edensor Littlewood e Srinivasa Ramanujan, atuou em Teoria de Números.

A frase aparece num livro que ele escreveu, chamado "A Apologia de um Matemático".

> "Eu acredito que a realidade matemática existe fora de nós, que nossa função é descobrir ou observá-la, e que os teoremas que provamos, e que descrevemos com grandiloqüência como nossas 'criações', são simplesmente notas de nossas observações."

Complemente o Estudo

Filmes

A Matemática não tem sido muito favorecida como tema de filmes. Mas, recentemente três filmes chamaram a atenção para temas matemáticos. É verdade que eles servem mais para diversão do que para nos informar sobre fatos, mas essa é a principal razão para se fazer filmes, não é mesmo?

No entanto, eles podem ser úteis como ponto de partida para discussões sobre temas de Matemática.

Nome do Filme: Enigma (2001)

Direção: Michael Apted

Sinopse: Em março de 1943, a equipe de elite dos decodificadores da Inglaterra tem uma responsabilidade monumental: decifrar o Enigma, um código ultra seguro utilizado pelos nazistas para enviar mensagens aos seus submarinos. Para liderar este trabalho é chamado um gênio da matemática que consegue realizar tarefas consideradas impossíveis pelos especialistas.

Nome do Filme: Uma Mente Brilhante (A Beautiful Mind) (2001)

Direção: Ron Howard

Sinopse: John Nash é um gênio da matemática que, aos 21 anos, formulou um teorema genial. Aos poucos ele se transforma em um sofrido e atormentado homem, que chega a ser diagnosticado como esquizofrênico. Após anos de luta para se recuperar, ele consegue retornar à sociedade e acaba recebendo o Prêmio Nobel de Economia em 1994.

Nome do Filme: Gênio Indomável (Good Will Hunting) (1997)

Direção: Gus Van Sant

Sinopse: Em Boston, um jovem de 20 anos, servente de uma universidade, revela-se um gênio em Matemática. Por determinação legal, precisa fazer tera-

pia, mas nada funciona, pois ele debocha de todos os analistas, até se identificar com um deles.

Neste filme você verá, como cenário, o MIT (Massachusetts Institute of Technology), um dos templos da ciência, e da Matemática, em particular.

Livros

A literatura de divulgação de temas matemáticos é rica, mas a publicação em português não é muito grande. No entanto, alguns livros se destacam.

Nome do Livro: A Experiência Matemática (1982)

Autores: Philip J. Davis e Reuben Hersh

Esse livro aborda diversos tópicos e contém bastante informação. Além disso, pode ser lido por partes, uma vez que suas seções são independentes.

Nome do Livro: O Último Teorema de Fermat (1998)

Autor: Simon Singh

O livro conta, de maneira empolgante, toda a trajetória de um grande problema de Matemática. É livro para ser lido em um único fôlego e relido, diversas vezes.

Nome do Livro: O Livro dos Códigos (2001)

Autor: Simon Singh

Desta vez o autor narra a história da Criptografia.

Nome do Livro: Número: A Linguagem da Ciência

Autor: Tobias Dantzig

Esse livro é difícil de achar pois está fora do prelo. Entretanto, se encontrado na biblioteca de algum amigo ou em alguma loja de livros usados pode dar muito prazer além de muita informação.

Sites

http://www-history.mcs.st-and.ac.uk/∼history/index.html.

Este site sobre História da Matemática é excelente.

http://mathworld.wolfram.com

Este site é uma enciclopédia de Matemática. Com a ferramenta de busca você poderá encontrar definições e teoremas sobre assuntos clássicos e atuais.

Solução de algumas atividades

Apresentamos, a seguir, a solução para as atividades propostas no módulo. Não incluímos todas por considerar que algumas não necessitam de gabarito. No entanto, se você tiver alguma dúvida, tanto nas respostas apresentadas, como na resolução das outras atividades, sugerimos que consulte a tutoria.

- Atividade 2

Como sabemos dividir um ângulo em dois, com régua e compasso, podemos dizer que sabemos construir certas "famílias" de polígonos. Por exemplo, o triângulo, assim como o hexágono, o dodecágono, e assim por diante. Também podemos construir o quadrado, o octógono, e assim por diante.

Como $\cos\left(\frac{2\pi}{5}\right) = -\frac{1}{4} + \frac{\sqrt{5}}{4}$, podemos construir o pentágono usando régua e compasso, assim como o decágono, o dodecágono, e assim por diante.

A lista parou por aqui, cerca de uns dois mil anos, até Gauss mostrar ser possível construir, com régua e compasso, o polígono de dezessete lados. Posteriormente, os polígonos com $(4^n + 1)$-lados foram agregados à lista dos que podem ser assim construídos.

- Atividade 5

31	26	
62	13	$/$
124	6	
248	3	$/$
496	1	$/$

Assim, segundo esse algoritmo, $31 \times 26 \ = \ 62 + 248 + 496 = 806$.

- Atividade 6

A tripla pitagórica gerada pelos números $u = 64$ e $v = 27$ é $(3456,\ 3367,\ 4825)$.

Os números 4601 e 6649 fazem parte da tripla pitagórica $(4800,\ 4601,\ 6649)$,

gerada pelos números $u = 32 = 2^5$ e $v = 75 = 3 \times 5^2$.

- Atividade 8

A decomposição em fatores primos de $12\,285$ é $3^3 \times 5 \times 7 \times 13$. A soma de seus divisores próprios é $14\,595$, o outro elemento do par de números amigáveis: $(12\,285,\ 14\,595)$.

- Atividade 10

$$\frac{1+\sqrt{5}}{2} \;=\; 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1+\ldots}}}}.$$

Por exemplo, $1 + 1/(1 + 1/(1 + 1/(1 + 1/(1 + 1/(1 + 1/(1 + 1)))))) = \frac{34}{21} \approx 1.619047619$. Uma *boa* aproximação de $\frac{1+\sqrt{5}}{2}$ é 1.618033989.

- Atividade 11

Não existe inteiro n tal que $\dfrac{1}{2^n} = 0$.

Sabemos que $1 + r + r^2 + r^3 + \ldots r^n \;=\; \dfrac{1 - r^{n+1}}{1 - r}$. Se $|r| < 1$, então $\displaystyle\sum_{i=0}^{\infty} r^n \;=\; \frac{1}{1-r}$.

- Atividade 12

Por exemplo, se $m < \sqrt{2}\,n$, então $m\sqrt{2} < 2\,n$. Basta multiplicar a primeira desigualdade por $\sqrt{2}$. Os gregos do tempo de Eudoxo não dispunham desse argumento. É possível comprovar a veracidade da afirmação usando um argumento geométrico. Veja, um quadrado de lado $n\sqrt{2}$ tem diagonal $2\,n$. Agora, se $m < \sqrt{2}\,n$, podemos desenhar um quadrado de lado m contido no quadrado de lado $\sqrt{2}\,n$ e sua diagonal $m\sqrt{2}$ é menor do que a diagonal do quadrado maior, que é $2\,n$.

- Atividade 14

$K = \dfrac{\pi}{4}$.

- Atividade 15

Os fatores primos de $3 \times 5 \times 7 + 1$ são 2 e 53, primos diferentes de 3, 5 e 7.

- Atividade 17

Conhecendo o volume v e a massa m da coroa, assim como as constantes γ e σ, podemos resolver a equação em x e descobrir quanto ouro e prata há nela sem destruí-la. Sabendo que $\gamma = 19\,300\text{kg/m}^3$ e $\sigma = 10\,500\text{kg/m}^3$, descubra o peso do ouro no caso da coroa ter volume $v = 0.15\text{m}^3$.

- Atividade 18

A próxima linha é 21, 23, 25, 27 e 29. Note que $21+23+25+27+29 = 125 = 5^3$.

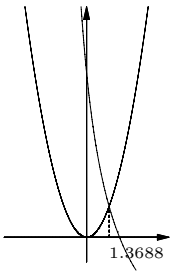
- Atividade 19

$64 = (3^2+2^2)\,(1^2+2^2) = (3\times1\pm2\times2)^2+(3\times2\mp2\times1)^2 \;=\; 49+16 \;=\; 1+64.$

- Atividade 20

Nem todas as propriedades das somas finitas são verdadeiras no caso das somas infinitas, como é o caso da propriedade distributiva.

- Atividade 22



Note que a hipérbole $(x+2)\,(y+10) = 40$ contém os pontos $(2,\,0)$ e $(0,\,10)$. A projeção do ponto comum sobre o eixo x ocorre entre 1.3 e 1.4.

- Atividade 23

Colocando numa equação, temos $x = x/6 + x/12 + x/7 + 5 + x/2 + 4$. A solução é $x = 84$.

- Atividade 24

A substituição $x = y - \frac{2}{3}$ transforma a equação $x^3 + 2x^2 + 10x = 20$ em $y^3 + \frac{26}{3}y = \frac{704}{27}$.

Fazendo $3st = \frac{26}{3}$ e $s^3 - t^3 = \frac{704}{27}$ chegamos à equação $t^6 + \frac{704}{27}t^3 - \frac{26^3}{27^2} = 0$, cuja solução *positiva* é $t^3 = \frac{-352+6\sqrt{3930}}{27}$. Assim, $s^3 = \frac{704}{27} + t^3 = \frac{352+6\sqrt{3930}}{27}$. Sabemos que $s - t$ é solução de $y^3 + \frac{26}{3}y = \frac{704}{27}$. Assim,

$$y = \frac{\sqrt[3]{352 + 6\sqrt{3930}} + \sqrt[3]{352 - 6\sqrt{3930}}}{3}.$$

Finalmente, $x = y - \frac{2}{3}$ leva à solução indicada na atividade.

- Atividade 25

Fazendo de conta que você não tenha notado que na equação $x^3 - 15x = 4$, $A = -15 < 0$, aplicamos a técnica de cálculo das raízes por radicais, fazendo $3st = -15$ e $s^3 - t^3 = 4$. Isso leva à equação $t^6 + 4t^3 + 125 = 0$, cujas raízes são $t^3 = -2 \pm \sqrt{-121} = -2 \pm 11\sqrt{-1}$.

Agora, os problemas. Primeiro, a raiz negativa. Se você não conhece a teoria dos números complexos, como era o caso de Cardano, pode seguir com a conta usando essa resposta *formal*. A outra possibilidade é que você a tome como um número complexo. De qualquer forma, como escolher t^3 positivo, como fizemos antes, se t^3 não é mais um número real? Neste caso, escolhemos qualquer um, digamos $t^3 = -2 + 11\sqrt{-1}$. Isso nos dá a $s^3 = 4 + t^3 = 2 + 11\sqrt{-1}$ e $s - t = \sqrt[3]{2 + 11\sqrt{-1}} + \sqrt[3]{2 - 11\sqrt{-1}}$ é uma *estranha* solução de $x^3 - 15x = 4$.

O mistério se desfaz ao observarmos que $(2 + \sqrt{-1})^3 = 2 + 11\sqrt{-1}$, assim como $(2 - \sqrt{-1})^3 = 2 - 11\sqrt{-1}$. Portanto,

$$s - t = \sqrt[3]{2 + 11\sqrt{-1}} + \sqrt[3]{2 - 11\sqrt{-1}} = 2 + 11\sqrt{-1} + 2 - 11\sqrt{-1} \;=\; 4$$

é apenas uma maneira um tanto diferente de escrever o número 4.

- Atividade 27

Uma sugestão consiste em arranjar a soma da maneira a seguir.

$$\begin{array}{ccccccccccccccc}
\frac{1}{2} & + & \frac{1}{4} & + & \frac{1}{8} & + & \frac{1}{16} & + & \frac{1}{32} & + & \frac{1}{64} & + & \dots & & \\
 & + & \frac{1}{4} & + & \frac{1}{8} & + & \frac{1}{16} & + & \frac{1}{32} & + & \frac{1}{64} & + & \dots & & \\
 & & & + & \frac{1}{8} & + & \frac{1}{16} & + & \frac{1}{32} & + & \frac{1}{64} & + & \dots & & \\
 & & & & & + & \frac{1}{16} & + & \frac{1}{32} & + & \frac{1}{64} & + & \dots & & \\
 & & & & & & & + & \frac{1}{32} & + & \frac{1}{64} & + & \dots & & \\
 & & & & & & & & & + & \frac{1}{64} & + & \dots & & \\
 & & & & & & & & & & & & & \vdots & \\
\hline
\frac{1}{2} & + & \frac{2}{4} & + & \frac{3}{8} & + & \frac{4}{16} & + & \frac{5}{32} & + & \frac{6}{64} & + & \dots & = &
\end{array}$$

A resposta é um número inteiro.

- Atividade 32

Aqui estão as três maneiras de escrever 99 como uma soma de quatro quadrados: $99 = 1 + 1 + 16 + 81 = 1 + 9 + 25 + 64 = 9 + 16 + 25 + 49$.

Você sabia que podemos escrever 98 de *quatro* maneiras diferentes como soma de quatro quadrados?

- Atividade 33

Essa é interessante. Faça $x^4 + 1 = (x^2 + ax + 1)(x^2 - ax + 1)$ e calcule a.

- Atividade 34

$4x \equiv 6 \mod 18$ tem duas soluções (residuais): 6 e 15; $4x \equiv 8 \mod 12$ tem quatro soluções: 2, 5, 8 e 11; $2x \equiv 7 \mod 13$ tem uma solução.

- Atividade 36

Por exemplo, $0, 1, -1, 2, -2, 3, -3, 4, -4, \ldots$.

- Atividade 37

A função $f(x) = \dfrac{c-d}{a-b}\,x + \dfrac{ad-bc}{a-b}$ estabelece uma bijeção entre os intervalos $(a,\, b)$ e $(c,\, d)$.

- Atividade 38

A função $f(x) = \operatorname{tg}\left(\dfrac{\pi}{2}\left(x - \dfrac{1}{2}\right)\right)$ estabelece uma bijeção entre o intervalo $(0,\, 1)$ e a reta real.

- Atividade 39

A linda frase que Paul Erdös usava para saudar seus amigos e colegas pesquisadores é "Minha mente está aberta".

- Atividade 40

$8^4 + 1 = 4097 = 17 \times 241$. Note que $17 = 2 \times 8 + 1$ e $241 = 30 \times 8 + 1$.

Referências

ANGLIN, W. S. *Mathematics:* A Concise History and Philosophy. New York: Springer Verlag, 1994.

BELL, E. T. *Men of Mathematics*. New York: Touchstone, 1965.

BOYER, C. B. *História da Matemática*. São Paulo: Edgar Blücher, 1974.

COURANT, R. e ROBBINS, H. *O que é Matemática?* Rio de Janeiro: Ciência Moderna, 2000.

COUTINHO, S. C. *Números Inteiros e Criptografia RSA*. Rio de Janeiro: IMPA / SBM, 1997.

DANTZIG, T. *Número:* A Linguagem da Ciência. Rio de Janeiro: Zahar, 1970

DAVIS, P. e HERSH, R. *A Experiência Matemática*. Rio de Janeiro: Francisco Alves, 1982.

DÖRRIE, H. *100 Great Problems of Elementary Mathematics:* Their History and Solution. New York: Dover, 1965.

EVES, H. *História da Matemática*. São Paulo: UNICAMP, 1996.

GRIFFITHS, H. B. e HILTON, P. J. *Matemática Clássica* – Uma Interpretação Contemporânea. São Paulo: Blücher / USP, 1975.3 v.

HEFEZ, A. *Curso de Álgebra*. v. 1. Rio de Janeiro: IMPA, 1997. (Coleção Matemática Universitária).

SANTOS, J. P. de O. *Introdução à Teoria de Números*. Rio de Janeiro: IMPA, 1998. (Coleção Matemática Universitária).

SINGH, S. *O Último Teorema de Fermat*. Rio de Janeiro: Record, 1998.

SINGH, S. *O Livro dos Códigos*. Rio de Janeiro: Record, 2001.

STRUIK, D. J. *A Concise History of Mathematics*. New York: Dover, 1987.