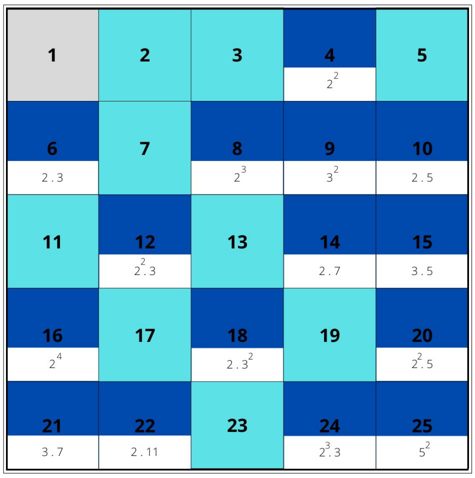
Boletim Lavrense de Matemática

Edição 10, 15 de outubro de 2022



O enigmático mundo dos números primos

O conceito de números primos parte das definições das operações básicas de multiplicação e divisão. No entanto, muitas perguntas sobre os primos permanecem sem resposta. Pode parecer estranho que ainda hoje, mais de 2000 anos depois dos primeiros registros sobre números primos de que se tem conhecimento, estudiosos estejam empenhados em responder perguntas referentes à existência e regularidade com que esses números surgem, mas a verdade é que muitas das tecnologias que usufruímos hoje dependem dos primos, seja direta ou indiretamente.

CURIOSIDADES

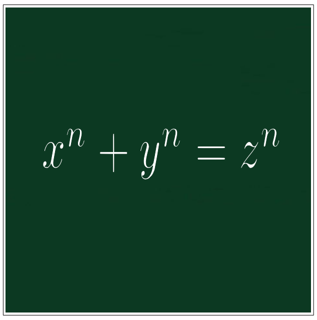
Quadrados mágicos

Algumas disposições de números naturais são bastante interessantes, e possuem propriedades muito intrigantes. O quadrado mágico é uma dessas curiosas disposições de números inteiros.

Na seção Curiosidades apresentamos as principais características de um quadrado mágico formado apenas por números primos.

Prêmio Wolfskehl

Premiações, em dinheiro, para pesquisadores que demonstram resultados importantes da Matemática não é algo incomum. Em 1908 a Academia de Ciências de Göttingen oficializou o Prêmio Wolfskehl, prêmio concedido pelo médico e matemático alemão Paul Wolfskehl (1856-1906) para aquele que provasse o Último Teorema de Fermat. O prêmio de 100.000 marcos alemães, segundo testamento de Wolfskehl, teria validade até 13 de setembro de 2007. Faltando pouco mais de 10 anos para o prêmio perder a validade, o matemático britânico Andrew Wiles, provou o tão intrigante teorema.



Índice

Contatos

Site: www.dmm.ufla.br/matematicaemtodolugar
e-mail: `boletimdamatematica.dmm@ufla.br`
Instagram: www.instagram.com/boletimlavrensedematematica

ESPECIAL

Números Primos

Para adentrar no fascinante mundo dos números primos é importante, antes de mais nada, entender alguns conceitos.

Chama-se números naturais os números 1, 2, 3, 4, 5, . . ., e assim por diante. Há uma infinidade de números naturais, porque é sempre possível somar 1 e obter mais um número natural.

Um número natural é chamado de número primo se a única maneira de escrevê-lo como uma multiplicação de dois números naturais for através da multiplicação dele próprio com o 1. Por exemplo, o número 11 é um número primo, porque ele só pode ser escrito como multiplicação de números naturais na forma

$$11 = 1 \cdot 11.$$

Já o número 12 não é primo, porque ele pode ser escrito como uma multiplicação de dois números naturais, ambos diferentes de 1, como pode-se ver a seguir

$$12 = 3 \cdot 4.$$

Quando um número natural não é primo, e é diferente de 1, ele é chamado de número composto. O número 1 não é primo e nem composto.

Observe que o conceito de número primo é tão simples que poderia ser facilmente ensinado a uma criança que conhece as operações básicas. Mas engana-se quem pensa que tal simplicidade se estende ao entendimento das características que esses números possuem.

Embora haja registros do estudo de números primos no século III, a.e.c., ainda hoje, em pleno século XXI, não existe um ser humano que tenha um completo entendimento desses números e suas características. Muitas questões continuam sem resposta. Mas é importante destacar que já há muito tempo é de conhecimento que números primos são os blocos de construção dos números naturais, os átomos da aritmética.

Em 1796, o matemático alemão Carl Friedrich Gauss (1777-1855) propôs e demonstrou o Teorema Fundamental da Aritmética, cujas propriedades já eram do conhecimento do matemático grego Euclides (300 a.e.c.) e estão enunciadas em seu famoso livro *Os Elementos*. O Teorema Fundamental da Aritmética afirma que todo número natural maior do que 1 ou é primo, ou pode ser escrito de modo único como uma multiplicação de números primos.

O processo de escrever um número como um produto de números primos é chamado de fatoração prima, ou simplesmente fatoração.

Por exemplo, os números 2 e 3 são números primos, os números 4 e 30 não são primos, mas podem ser fatorados como pode-se ver nas seguintes multiplicações

$$4 = 2 \cdot 2$$

$$30 = 2 \cdot 3 \cdot 5.$$

Muitos sistemas modernos de criptografia[1], sistemas que são usados para criptografar e descriptografar mensagens secretas, dependem da identificação de números primos e do problema de fatorar números compostos. Uma fatoração muito famosa foi o teste para o sistema criptográfico RSA. O desafio era fatorar um número de 129 dígitos, conhecido como RSA129. Esse desafio foi proposto em 1977, e algumas pessoas projetaram 40 quatrilhões de anos para que o RSA129 fosse fatorado. No entanto, em 1994 o desafio foi solucionado e ao ser fatorado o número RSA129 revelou a mensagem secreta: *"The magic words are squeamish ossifrage"*(As palavras mágicas são abutre melindroso).

Números primos surgem também na Biologia. Algumas espécies de cigarras têm ciclos de vida primos. Ciclo de vida é o conjunto de transformações pelas quais os indivíduos da espécie podem passar para assegurar a sua continuidade. Cientistas identificaram ciclos de vida de 13 e 17 anos, o que para insetos são considerados ciclos bastante longos. Acredita-se que os números primos 13 e 17 foram selecionados no processo evolutivo porque esses ciclos eram menos propensos a emergir, hibridizar e quebrar com outros ciclos sincronizados, como o acasalamento.

Na Biologia Molecular cientistas inferem que certas sequências de aminoácidos no material genético exibem padrões esperados de números primos. O material genético compõe um código, chamado código genético, responsável por resguardar as informações necessárias ao desenvolvimento do organismo que o possui, mas também permite que evolução e seleção natural ocorram. A especificidade combinatória dos aminoácidos permite traduzir as propriedades de codificação nas propriedades dos números e vice-versa. Há uma equivalência entre os números primos menores que 64 e os equivalentes numéricos dos aminoácidos. É interessante notar que, exceto pelos primos 2 e 3, os demais números primos menores que 64 são da forma $4n + 1$ ou $4n + 3$, com n sendo um número natural.

Existem muitas outras áreas do conhecimento onde a teoria de números primos é utilizada. E também há muitas informações interessantes referentes à esses números. A própria denominação *números primos* gera muita curiosidade. Acredita-se que tal denominação surgiu com os pitagóricos que dividiam os números naturais em três classes, uma classe formada pelo número 1, chamado unidade, uma segunda classe formada pelos números que não podem ser gerados por multiplicação, os quais eram chamados de números primários ou primos, e a terceira classe formada pelos números que podem ser gerados por um processo que multiplicação, os quais eram chamados números secundários, e hoje são conhecidos como números compostos.

Com relação à quantidade de números primos existentes, Euclides mostrou, no século III a.e.c., que existem infinitos números primos. Mas outras perguntas persistem. Como encontrar os números primos? Existe algum processo ou fórmula que possa

[1]Veja a Edição 9 do Boletim Lavrense de Matemática

determinar tais números?

O matemático grego e bibliotecário da famosa Biblioteca de Alexandria, Eratóstenes (276-194 a.e.c.), inventou uma técnica para encontrar os números primos, conhecida hoje como Crivo de Eratóstenes. É uma técnica simples e segue as seguintes etapas: liste os números naturais de 1 até um certo número N e, em seguida, risque a partir do número 2 todos os números de dois em dois (ou seja, os múltiplos de 2 exceto o próprio 2); como 3 é maior do que 2 e não foi riscado, mantenha o 3 e risque os números de três em três, a partir do 3 (ou seja, os múltiplos de 3 exceto o próprio 3); 5 é o próximo número ainda não riscado, então deixe 5 e risque a partir do 5 os números de cinco em cinco, e assim por diante. Todos os números naturais, diferentes de 1, que não foram riscados nesse processo formam o conjunto de todos os números primos menores ou iguais a N. Na figura abaixo, os números primos estão em blocos na cor laranja e os compostos em blocos azuis.

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	100

Crivo de Eratóstenes com $N = 100$

Não existe uma fórmula simples e eficiente para determinar primos. Mas existem muitas tentativas de se criar tal fórmula. Poderia-se pensar numa fórmula que produz todos os primos em ordem crescente, e nesse caso poderia-se aplicar a fórmula para obter o enésimo número primo. Outra possibilidade seria uma expressão que gere apenas números primos.

Esse segundo tipo de fórmula foi pensado por muitos estudiosos. Para citar alguns exemplos, no século XVII, Pierre de Fermat (1601-1665) afirmou que

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

é primo para todo número natural, no entanto, no século XVIII Leonhard Euler (1707-1783) mostrou que para $n = 5$ tal conjectura[2] falha. Em 1772 Euler descobriu a fórmula

$$n^2 - n + 41$$

que gera primos para n de 1 até 40; em 1798, Adrien-Marie Legendre (1752-1833) observou que a expressão

$$n^2 + n + 41$$

produz primos para n de 1 até 39.

Fórmulas que produzem apenas números primos muitas vezes levam tempo para serem refutadas porque geralmente produzem primos por um tempo e depois falham. Isso ocorre porque há um número considerável de primos entre os menores números naturais.

Outra questão bastante investigada é a distribuição dos números primos, ou ainda, a diferença entre dois primos consecutivos. Por exemplo, ao considerar os dez menores números primos

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29$$

é possível ver que a diferença entre dois primos consecutivos será

$$1, 2, 2, 4, 2, 4, 2, 4, 6.$$

Denotando por p_n e p_{n+1} dois primos consecutivos, e por d_n a diferença entre eles,

$$d_n = p_{n+1} - p_n,$$

sabe-se que para $p_n > 2$, d_n é um número par. Porém, não se sabe ainda se todo número par é uma diferença entre primos.

Com base em tabelas de números primos, Legendre conjecturou em 1797 um importante resultado sobre a distribuição dos números primos. O resultado hoje conhecido por Teorema dos Números Primos afirma que "O número de primos menores ou iguais a n é aproximadamente $\dfrac{n}{\ln n}$. Este resultado foi demonstrado independentemente pelos matemáticos Jacques Hadamard e Charles-Jean de La Vallée, em 1896.

Em 1849, o matemático francês Alphonse de Polignac conjecturou que "Dado k um número natural, existem infinitos pares de primos consecutivos cuja diferença é igual a $2k$." Alguns avanços já foram feitos em relação à conjectura de Polignac. No entanto, esse continua sendo um problema aberto uma vez que não foi provado e nem refutado. Um caso particular da conjectura de Polignac é o caso em que $k = 1$, ou seja, quando p e $p + 2$ são primos. Quando a diferença entre dois primos consecutivos é igual a 2, diz-se que p e $p + 2$ são primos gêmeos. Os menores pares de primos gêmeos são $(3, 5)$, $(5, 7)$, $(11, 13)$. Em 1949, o matemático P. A. Clement caracterizou os primos gêmeos da seguinte forma: "Para $p \geq 2$, os naturais p e $p + 2$ são ambos primos se e somente se $p(p+2)$ divide $4[(p-1)! + 1] + p$." Embora bastante interessante, a caracterização não serve para determinar primos gêmeos. Os maiores pares de primos gêmeos já encontrados possuem um número de dígitos que ultrapassa 100.000.

Outra conjectura, bem mais recente, é devida ao matemático romeno Dorin Andrica. Andrica conjecturou que: "Para todo número natural n,

$$\sqrt{p_{n+1}} - \sqrt{p_n} < 1$$

onde p_n denota o enésimo número primo." Embora pareça verdadeira, tal conjectura nunca foi provada.

Existem muitas outras conjecturas e resultados já provados sobre números primos. Segue abaixo referências onde um vasto conteúdo sobre os primos pode ser encontrado.

Referências:

Introdução à história da matemática, Howard Eves. Unicamp, 2004.

Números Primos: Velhos mistérios e novos recordes, Paulo Ribenboim. IMPA, 2012.

Prime numbers: A computational perspective, Richard Crandall, Carl Pomerance. Springer, 2000.

Prime numbers: The most mysterious figures in math, David Wells. Wiley, 2005.

■

[2] Uma conjectura é uma afirmação matemática não provada.

O Último Teorema de Fermat

Pierre de Fermat, um dos grandes contribuidores para o desenvolvimento e fundamentação do cálculo diferencial e integral, nasceu em Beaumont de Lomagne (França) em 1601. Foi um advogado discreto que se pautou pelo cumprimento do dever. Para ele, a matemática era um lazer, uma espécie de divertimento sério, que lhe permitia dar vazão às ideias profundas ligadas ao desenvolvimento da cultura de sua época. Durante sua vida manteve correspondência com muitos dos principais matemáticos de seu tempo, como Blaise Pascal e Marin Mersenne.

Pierre de Fermat
Fonte: *Wikipedia*

Fermat possuía um verdadeiro horror às demonstrações matemáticas muito longas, seus trabalhos resumiam-se a poucas linhas, frequentemente escritas à margem de livros que manuseava. Ficou conhecido como o "Príncipe dos Amadores" por ter descoberto as leis da probabilidade, os fundamentos do cálculo diferencial e elegantes e difíceis teoremas sobre números inteiros. Fermat não se preocupou em publicar seus estudos, cópias manuscritas de seus trabalhos circulavam nas mãos de seus discípulos e amigos. Coube a seu filho, Clément-Samuel, reunir algumas de suas brilhantes conclusões e publicá-las numa compilação intitulada *Varia Opera Mathematica*, em 1679. O mais famoso trabalho de Fermat é conhecido como o seu Último Teorema, no qual afirmou que a equação

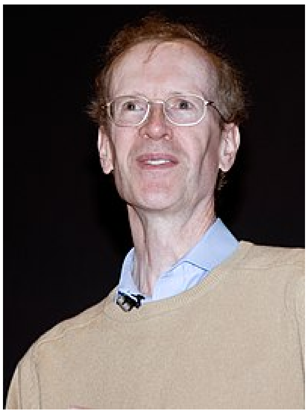
$$x^n + y^n = z^n$$

não tem solução inteira positiva para $n > 2$. A propósito da demonstração deste teorema, escreveu à margem de um exemplar da obra de Diofanto: *"Encontrei uma demonstração verdadeiramente admirável, mas a margem é muito pequena para apresentá-la. Sinto muito."*

Desde então muitas gerações de matemáticos foram envolvidas nesta batalha de cerca de 350 anos. Batalha esta que influenciou, praticamente, todas as áreas da Matemática. Porém em 1994, o inglês Andrew Wiles, professor da Universidade de Oxford, demonstrou com a ajuda do matemático Richard Taylor, o Último Teorema de Fermat.

Para Wiles o problema mais famoso da Matemática nestes últimos quatro séculos tornou-se uma obsessão desde quando, aos 10 anos de idade, pôs as mãos no livro de Eric Temple Bell, *"O Último Problema"*.

Embora o problema parecesse tão simples, durante quatro séculos, os grandes matemáticos não puderam provar e nem refutar a afirmação de Fermat, assim, Wiles achou que tinha que ser ele a resolvê-lo.



Andrew Wiles
Fonte: *Wikipedia*

A história dos detalhes de como esta afirmação se tornou a mais terrível provocação de Fermat é magistralmente contada por Simon Singh em seu livro *"O Enigma de Fermat"*, edição americana, ou *"O Último Teorema do Fermat"*, edição inglesa. O livro de Singh tornou-se o livro mais vendido no mundo sobre o assunto e fez Wiles ficar conhecido fora de seu círculo acadêmico.

Sobre a evolução da demonstração do Último Teorema de Fermat, segue uma pequena cronologia: de Fermat, conhece-se apenas um esboço de demonstração para $n = 4$. Euler conseguiu uma demonstração para $n = 3$ e o caso $n = 5$ foi provado por Dirichlet, em 1828 e por Legendre, em 1830. Em 1832, Dirichlet provou o resultado para $n = 14$ e em 1839, Gabriel Lamé sugeriu uma demonstração para $n = 7$, mas não estava completamente certa. Sophie Germain provou que se n é primo ímpar menor que 100, a equação não tem solução em naturais não divisíveis por n. Kummer demonstrou o teorema para expoentes n que são primos regulares (inclui todos os primos menores que 100 exceto o 37, 59, 67). Em 1980, Wagstaff mostrou que o teorema é válido para todo n até 125.000. Em 1983, Gerd Faltings descobriu que para todo $n > 3$, se existirem soluções da equação de Fermat, estas são em número finito e mais tarde, Heath-Brown provou que a proporção de naturais n para os quais a equação não tem soluções, tende para 100% quando n aumenta. No dia 23 de junho de 1993, após sete anos de trabalho, Wiles anunciou, numa conferência do *Sir Isaac Newton Institute for Mathematical Sciences* em Cambridge, ter encontrado uma demonstração para o resultado enunciado por Fermat mas, pouco tempo depois, foi verificada uma pequena falha. Wiles retirou-se durante mais um ano e, finalmente, retornou com a demonstração reformulada.

Em novembro de 1994, depois de alguns meses de apreciação das 200 páginas, a demonstração de Wiles foi definitivamente aceita. Trata-se de uma demonstração de tal forma técnica que apenas algumas dezenas de matemáticos em todo o mundo estarão em condições de seguir o raciocínio. Em 1997, Wiles recebeu o *Wolfskehl Prize*, o mais honroso prêmio entre todos os outros que recebeu ou ainda receberá pela solução do problema mais famoso da Matemática nestes últimos quatro séculos. Usando uma demonstração de formalismo elaborado, o inglês conseguiu provar que Fermat estava correto. A façanha rendeu ao matemático não apenas fama, mas uma dúzia de prêmios importantes na área.

Referências:

www.webpages.ciencias.ulisboa.pt
www.g1.globo.com
www.angelfire.com ■

CURIOSIDADES

Quadrado mágico primo com bordas

Um quadrado mágico de ordem n é uma disposição quadrada de n^2 números naturais distintos, distribuídos de modo que a soma de todos os números de uma mesma linha, de uma mesma coluna ou da diagonal principal resultam no mesmo valor, chamado *constante mágica* do quadrado.

O mais antigo quadrado mágico de que se tem conhecimento é chamado de *lo-shu*. O *lo-shu* é parte do legado das antigas tradições chinesas de matemática e divindade.

Allan Johnson Jr. descobriu um quadrado mágico 7×7 composto inteiramente de números primos. A constante mágica do quadrado 7×7 é 13.853. Note que os quadrados concêntricos menores, 3×3 e 5×5, também são mágicos e tem constantes mágicas, 5.937 e 9.895, respectivamente.

Referência:

Incríveis passatempos matemáticos, Ian Stewart. Zahar, 2009. ■

2777	1409	2339	1481	1061	2699	2087
2531	1889	2237	2459	1229	2081	1427
1367	2357	2399	1511	2027	1601	2591
2909	1031	1607	1979	2351	2927	1049
1301	2741	1931	2447	1559	1217	2657
1097	1877	1721	1499	2729	2069	2861
1871	2549	1619	2477	2897	1259	1181

DESAFIOS

Desafios da Edição

Envie sua resolução dos desafios desta seção para nosso e-mail. A mais criativa será divulgada na próxima edição do Boletim.

1) Considere um conjunto de 10 cartas numeradas de 1 a 10. Organize todas as cartas em um círculo de forma que a soma de cada duas cartas consecutivas seja um número primo.

2) Conjectura de Golbach: Todo número par maior que 2 é a soma de dois números primos. Por exemplo:

$$6 = 3 + 3$$

$$10 = 5 + 5$$

$$10 = 7 + 3$$

Em 1742 o matemático Christian Goldbach (1690-1764) propôs essa conjectura, que não funciona para números ímpares. Ainda não se conhece um número par que não seja a soma de dois números primos. Com o uso de computadores os matemáticos já verificaram até o número $6 \cdot 10^{16}$. Isso não significa que a conjectura esteja provada.

Desafio: De quantas maneiras diferentes podemos escrever o número 100 como a soma de dois números primos?

Referências:

Ideias Geniais na matemática: maravilhas, curiosidades, enigmas e soluções brilhantes da mais fascinante das ciências, Surendra Verma. Gutenberg, 2014.
Quebra-cabeças de Matemática, quebracabecas@obmep.org.br

Respostas dos desafios da edição anterior (acesse aqui a 9ª edição)

Desafio 1: ENIGMA, chave: Turing.

Desafio 2: Basta mover a torre branca quatro casas para a esquerda. ■

Participação

O Boletim Lavrense de Matemática quer ouvir você. Envie-nos sugestões de reportagem, sua opinião, correções e dúvidas através de nosso e-mail.