Matemática Universitária Nº 14, dezembro de 1992, 29–46

Os Recordes dos Números Primos*

Paulo Ribenboim

Toda pessoa tem uma admiração natural pelos recordes. Eles exercem fascinação e excitam a imaginação. O célebre *Livro Guinness de Recordes*, que teve uma quantidade surpreendente de edições, está repleto de informações e de fatos, os mais curiosos e interessantes.

Vocês sabiam que o mais longo percurso em bicicleta foi realizado por Carlos Vieira, de Leiria, Portugal? Que ele pedalou, sem parar, durante 91 horas, percorrendo uma distância de 2.407 km, de 8 a 16 de junho de 1983?

Vocês sabiam que a maior pedra retirada de um corpo humano pesava 6,290 kg? Que a pessoa era uma senhora de 80 anos e que este fato se passou em Londres em 1952?

E, agora, um fato que nos interessa mais de perto: HIDEAKI TOMOYOKI, nascido em Yokohama, em 1932, recitou de memória 40.000 decimais do número real π. Ele levou 17 horas e 20 minutos para realizar sua façanha com interrupções que totalizaram 4 horas.

Ao percorrer o *Livro Guinnes de Recordes* nota-se que ele contém poucos recordes científicos e menos ainda sobre números.

Vocês sabem, talvez, que eu escrevi um livro intitulado *O Livro dos Recordes dos Números Primos*, que tem por objetivo expor os recordes e as façanhas dos matemáticos neste domínio abandonado pelo Guinness.

A história em torno deste livro merece ser contada. Após ter sugerido, à minha universidade, a organização de uma série de

* Traduzido do francês pelo Professor Antônio Paques, a quem os editores consignam aqui seus agradecimentos.

aulas especiais para os estudantes dos primeiros anos de estudos, eu devia fazer-lhes uma palestra sobre um assunto que fosse ao mesmo tempo acessível e muito atraente. A idéia que me ocorreu foi de falar sobre os recordes dos números primos, o que, em sua essência, se aproxima das façanhas atléticas, sexuais e outras.

O interesse mostrado pelos estudantes foi bem superior à minha expectativa. Decidi então escrever um texto baseado nesta minha palestra. De início curto, em seguida cada vez mais longo à medida que tomava conhecimento de novos fatos e recordes. As numerosas e úteis sugestões de meus colegas permitiram-me completar minha obra, da qual existe uma versão resumida, traduzida em francês e publicada pelas Presses Universitaires de France.

Devo confessar de imediato que, no momento de minha palestra para os estudantes, eu conhecia somente uns poucos teoremas e recordes de números primos. Para mim esses fatos, interessantes por si mesmos, não se encontravam ligados uns aos outros e apareciam como teoremas isolados. Não era claro como eles faziam parte de uma mesma teoria.

Se devia escrever um livro, minha primeira tarefa seria organizar aquilo que eu deveria apresentar em uma teoria coerente.

É sabido que, em poucas palavras, o método científico consiste em dois processos:

1) a observação, a experimentação — *a análise*
2) a formulação das leis e teoremas e a organização dos conhecimentos — *a síntese.*

Minha tarefa podia ser assim definida: *a síntese dos fatos conhecidos sobre os números primos, com uma ênfase sobre os recordes.*

A originalidade de meu trabalho seria, sem dúvida, a exploração sistemática da interface cálculo-teoria.

Não havia necessidade de justificar esse estudo; ninguém ignora o papel dos números primos na teoria dos números. De fato, o teorema fundamental da aritmética afirma que todo número inteiro $n > 1$ se escreve de modo único (a menos da ordem dos fatores) como produto de números primos. Os números primos são, portanto, como as pedras de base sobre as quais se apoia o edifício da aritmética.

Como organizar a teoria dos números primos?

Explico essa questão por meio de questões naturais e bem definidas que se impõem uma após a outra:

I) Quantos são os números primos?
II) Como produzir números primos?
III) Como reconhecer se um dado número é primo?
IV) Onde encontrar os números primos?

Outros capítulos da teoria devem ser dedicados aos seguintes estudos:

V) Os tipos especiais de números primos.
VI) Experimentação e heurística.

No que diz respeito à seção 1, direi que existe uma infinidade de números primos e indicarei as demonstrações. Por causa de sua natureza indireta, subsiste o problema da produção ou geração dos números primos, que discutirei na seção 2.

Uma questão muito em voga atualmente diz respeito ao reconhecimento dos números que são primos. Este é o assunto da seção 3.

Na seção 4, dedicada à distribuição dos números primos entre os números inteiros, encontram-se os teoremas mais profundos da teoria.

Não me estenderei sobre as seções 5 e 6, as quais merecem uma atenção maior e tornariam esta exposição excessivamente longa.

1. Quantos são os números primos.

Como é sabido, é devido a EUCLIDES a demonstração, que se encontra em seus *Elementos*, da existência de uma infinidade de números primos. Vejamos a demonstração de EUCLIDES:

Se p é o maior número primo, seja

$$p^{\#} + 1 = (\prod_{q \leq p} q) + 1$$

(produto dos primos $q \leq p$, mais 1)

Dois casos são possíveis:

a) ou $p^{\#} + 1$ é primo e, neste caso, existiria um primo maior que p,
b) ou $p^{\#} + 1$ não é primo.

Neste segundo caso um divisor primo de $p^{\#} + 1$ não poderia ser igual a nenhum dos primos $q \leq p$ e portanto ele seria maior que p.

Em ambos os casos a hipótese que p seja o maior número primo leva a uma conclusão absurda. Isto mostra que existe, necessariamente, uma infinidade de números primos.

É necessário observar que esta demonstração indireta não permite deduzir um método de geração de números primos. Contudo, a questão seguinte se impõe naturalmente:

Existe uma infinidade de números primos p tais que $p^{\#} + 1$ seja primo?

Muitos cálculos feitos por muitos matemáticos foram dedicados a esta questão.

RECORDE: O maior primo p conhecido, tal que $p^{\#} + 1$ é primo, é $p = 13649$; $p^{\#} + 1$ tem 5862 algarismos. Ele foi calculado por H. DUBNER em 1987.

Existem outras demonstrações da existência de uma infinidade de números primos; cada uma delas revela um aspecto interessante do conjunto dos números primos.

EULER demonstrou:

$$\sum \frac{1}{p} = \infty$$

(soma dos inversos de todos os números primos)

Portanto, não poderia existir somente um número finito de números primos.

Esta demonstração se encontra em muitos livros elementares da teoria de números ou da análise real.

Um comentário interessante: para todo $\epsilon > 0$, tão pequeno quanto se deseje, tem-se

$$\sum_{n=1}^{\infty} \frac{1}{n^{1+\epsilon}} < \infty$$

De alguma forma, isto poderia ser interpretado dizendo-se que os números primos estão dispostos mais próximos uns dos outros, ou de modo menos disperso, que os números da forma $n^{1+\epsilon}$ (por exemplo, os números $\frac{1}{n^2}$, cuja soma, calculada por Euler, é $\frac{\pi^2}{6}$).

POLYA também fez uma demonstração muito simples e elegante da existência de uma infinidade de números primos.

É suficiente encontrar uma seqüência infinita de números naturais, dois a dois relativamente primos, sem recorrer, evidentemente, à existência de uma infinidade de números primos — fato que se quer justamente estabelecer.

A seqüência dos números de FERMAT $F_n = 2^{2^n} + 1$ (para $n = 0, 1, 2, \cdots$) goza dessa propiedade, como pode ser facilmente verificado. Portanto, se p_n é um número primo que divide F_n, então os números primos p_n são dois a dois distintos.

Tratarei os números de FERMAT com mais atenção na seção 3.

2. A produção de números primos.

O problema consiste em encontrar uma "boa" função $f: N \rightarrow \{\text{primos}\}$. Deseja-se que essa função f seja, na medida do possível, fácil de calcular e que ela possa ser expressa, de preferência, por meio de funções já bem conhecidas.

Deve-se também impor condições sobre essa função.

Por exemplo:

Condição (a): $f(n)$ é igual ao n-ésimo primo (em ordem crescente); isto dará uma "fórmula" para o n-ésimo número primo.

Condição (b): se $n \neq m$ então $f(n) \neq f(m)$; isto dará uma função geradora de números primos, mas não necessariamente todos os números primos.

Condição (c): o conjunto dos números primos coincide com o conjunto dos valores positivos da função; esta é uma exigência não muito rigorosa e que será possível de ser satisfeita, de uma forma surpreendente, como veremos mais tarde.

Para começar discutiremos as fórmulas para o n-ésimo número primo. Existem muitas! De fato, muitos dentre nós, em nossa juventude, já tentamos algumas vezes, e com sucesso, obter uma fórmula para o n-ésimo número primo. Infelizmente, todas essas fórmulas têm um aspecto em comum: elas expressam o n-ésimo primo utilizando-se de funções dos números primos precedentes, as quais são difíceis de calcular. Portanto essas fórmulas não têm sido úteis para descrever propriedades dos números primos.

Mesmo assim desejo citar, à título de ilustração, uma dessas fórmulas. Ela é devida à J.M. GANDI (1971), um matemático falecido prematuramente e que trabalhou também sobre o último teorema de Fermat — faço isto como uma homenagem à sua memória.

A fórmula é:

$$p_n = [1 - \log\log(\frac{1}{2} + S_n)], \text{ onde}$$

$$S_n = \sum_{r=1}^{n} \frac{(-1)^r}{2^{p_{i_1}\cdots p_{i_r}} - 1}$$

e $1 \leq i_1 < i_2 < \cdots < i_r \leq n-1$, com $p_1 = 2, p_2 = 3, \cdots$ sendo a seqüência dos números primos (em ordem crescente).

Vê-se como seria penoso calcular p_n.

Apresentarei agora uma função geradora de números primos. E.M. WRIGHT (co-autor junto com G.H. HARDY do célebre livro sobre a teoria dos números) mostrou que:

se $\omega = 1,9287800\cdots$ então

$$f(n) = [2^{2^{\cdot^{\cdot^{\cdot^{w}}}}}] \qquad \text{(com } n \text{ "dois")}$$

é igual a um número primo, para todo $n \geq 1$. Assim $f(1) = 3$, $f(2) = 13$, $f(3) = 16381$, enquanto que $f(4)$ seria muito difícil de calcular e teria mais de 5.000 algarismos decimais. Por outro lado, a determinação exata de w depende, em última análise, do conhecimento dos números primos, o que faz com que esta fórmula seja desprovida de interesse.

Poder-se-ia perguntar se não existem funções geradoras de primos que sejam mais simples. Por que não polinômios?

Porque tem-se o resultado negativo seguinte:

Se $f \in Z[X_1, \cdots, X_m]$, existe uma infinidade de m-uplas de inteiros $(n_1, \cdots, n_m)$ tais que $|f(n_1, \cdots, n_m)|$ é um número composto.

Existem outros resultados negativos do gênero.

Ao contrário, pode-se perguntar se existem polinômios, mesmo a uma variável, tendo muitos valores sucessivos que sejam números primos. Mais especificamente, dado um número q, pode-se perguntar se é possível encontrar um polinômio de grau 1, isto é, do tipo $f_q(X) = dX + q$, tal que seus valores em $0, 1, \cdots, q-1$ sejam números primos — isto produz uma sequência de q primos em progressão aritmética de razão d e termo inicial q.

Para pequenos valores de q, é muito fácil:

q	d		valores					
2	1	2	3					
3	2	3	5	7				
5	6	5	11	17	23	29		
7	150	7	157	307	...	...	...	907

Não se sabe demonstrar que isto é possível para todo número primo q.

A seguir damos os recordes sobre esta questão.

RECORDE: Em 1986, G. LÖH deu os menores valores de d quando $q = 11, 13$:

$q = 11$ dá $d = 1536160080$

$q = 13$ dá $d = 9918821194590$

Pode-se considerar também a questão análoga da existência de seqüencias longas de números primos em progressão aritmética.

RECORDE: A mais longa seqüência conhecida de primos em progressão aritmética consiste de 20 termos, o primeiro é $a = 214861583621$ e a razão é $d = 18846497670$. Descobertas de J. YOUNG e J. FRY em 1987.

EULER decobriu polinômios quadráticos com muitos valores números primos. Precisamente, ele observou que se q é um número primo, a saber, $q = 2, 3, 5, 11, 17$, ou 41, então o polinônio $f_q(X) = X^2 + X + q$ é tal que $f_q(0), f_q(1), \cdots, f_q(q-2)$ são números primos (evidentemente, $f_q(q-1) = q^2$ não sendo primo, a seqüência de valores primos sucessivos é a melhor que se pode esperar). Assim, obtém-se 40 números primos quando $q = 41 : 41, 43, 47, 53, \cdots, 1447, 1523, 1601$.

Pode-se encontrar números primos $q > 41$ com a propriedade indicada? É uma questão muito natural. A existência de uma infinidade de tais primos q permitiria gerar sequências arbritariamente longas de números primos.

Mas o teorema seguinte diz justamente que este não é o caso:

TEOREMA. *Seja q um número primo.*

1) RABINOVITCH mostrou em 1912 que os inteiros $f_q(0), f_q(1), \cdots, f_q(q-2)$ são todos primos se e somente se o corpo quadrático imaginário $Q[\sqrt{1-4q}]$ tem um número de classes igual a 1.

2) Em 1966 BAKER e STARK determinaram, independentemente e sem sombra de dúvida (que pairava sobre o trabalho de HEEGNER em 1952), todos os corpos quadráticos imaginários com um número de classes igual a 1.

Como uma conseqüência desse resultado tem-se que o número de classes de $Q(\sqrt{1-4q})$ é 1 se e somente se $4q-1 = 7$, 11, 19, 43, 67 ou 163, ou seja, $q = 2$, 3, 5, 11, 17 ou 41.

Assim se chega ao *recorde absoluto* (que não poderá jamais ser ultrapassado) seguinte:

RECORDE: $q = 41$ é o maior número primo tal que $f_q(0), f_q(1), \cdots, f_q(q-2)$ são números primos.

É interessante observar que para a resolução de um problema aparentemente inocente como este tenha havido necessidade de recorrer a teorias bastante sofisticadas. Os detalhes dessa resolução podem ser vistos em meu artigo *Euler's famous prime generating polynomial and the class number of imaginary quadratic fields* (L'Enseignement Mathématique 34 (1988), 23–42)

Agora, voltamos nossa atenção para os polinômios cujos valores positivos constituem o conjunto dos números primos. Sua existência, muito surprendente, foi descoberta por Yu. V. MATIJASEVIC. em 1971 e tem ligação com o 10º problema de HILBERT. Explicitando-se a demonstração de MATIJASEVIC, é possível indicar concretamente tais polinômios. A seguir damos os recordes, os quais dependem do número de indeterminadas n e do grau d.

Recorde			
n	d	Ano	
26	25	1976	J.P.JONES, D.SATO, H.WADA e D.WIENS
45	5	1976	(não explícito)
	(mínimo)		
10	$1,6 \times 10^{48}$	1977	YU. V. MATIJASEVIC
(mínimo)			(não explícito)

3. O reconhecimento dos números primos.

É preciso que se diga imediatamente: dado um número natural N qualquer, é possível reconhecer, efetuando-se um número finito de operações, se o número N é primo. De fato, é suficiente dividir sucessivamente N por cada um dos números $d, 1 < d < N$

— aliás, é suficiente limitar-se às divisões de N pelos números primos d tais que $d^2 < N$. Se em cada divisão obtém-se um resto não nulo, então N é primo. O problema com este método é que o número de operações torna-se considerável se N é muito grande.

Procura-se então encontrar um algorítmo A, cujo número de operações efetuadas sobre os algarismos de N permaneça limitado por uma função f_A que não cresça rapidamente com N, ou seja, $f_A(N)$ é limitado por um polinômio no número de algarismos $1 + [\log_{10} N]$ de N

Este problema ainda continua aberto, isto é, não é sabido se um tal algorítmo a tempo polinomial pode existir, pois ainda não foi demonstrada a impossibilidade como também, por outro lado, um tal algorítmo (se existir) permanece por ser descoberto.

Os esforços nessa direção levaram à vários tipos de algorítmos:

- algorítmos para números arbitrários
- algorítmos para números de forma especial
- algorítmos justificados
- algorítmos baseados em conjecturas
- algorítmos deterministas
- algorítmos probabilísticos

Explicamos a seguir esses termos, ilustrando-os através de exemplos.

Entre os algorítmos aplicáveis a números arbitrários, citamos inicialmente o algorítmo de MILLER (1975) cuja justificativa requer a hipótese generalizada de RIEMANN. Para este algorítmo $f_A(N) \leq C(\log N)^5$ (onde $C > 0$ é uma constante); trata-se portanto de um logorítmo não justificado a tempo polinomial.

O algorítmo de ADLEMAN, POMERANCE E RUMELY (1983) está completamente justificado e o número de operações sobre os algarismos é limitado por $(\log N)^{C \log\log\log N}$ (C constante). Este algorítmo na prática, não está longe de ser a tempo polinomial e ele se aplica a números arbitrários.

Os dois algorítmos precedentes são deterministas, ao contrário daqueles que vamos considerar agora.

Para isso é necessário considerar os números pseudo-primos. Seja a um inteiro, $a > 1$. Se p é um número primo então, pelo

pequeno teorema de FERMAT, $a^{p-1} \equiv$ (mod p). Por outro lado, um número $N > 1$ tal que $a^{N-1} \equiv 1 \pmod{N}$ pode muito bem ser composto e, neste caso, N é chamado um *pseudo-primo na base a* (e denotado por $psp(a)$). Por exemplo, 341 é o menor psp (2).

Na realidade, existe uma infinidade de números pseudo-primos na base $a > 1$.

Entre os números pseudo-primos na base a existem aqueles, chamados *fortemente pseudo-primos na base a*, que verificam uma certa propriedade suplementar; estes também existem em número infinito.

Um algorítmo A é dito *probabilístico* (ou um teste probabilístico de primalidade) se a aplicação de A ao número N indicar que N é composto ou que, com uma forte probabilidade, N é primo.

Entre os testes desse tipo, mencionamos aqueles de BAILLIE e WAGSIAFF, de SOLOVAY e STRASSEN e de RABIN. O primeiro, à exemplo dos outros, recorre aos números " testemunhas". Seja $k > 1$ (por exemplo $k = 30$). Sejam $a_1 = 2, a_2 = 3 \cdots, a_k$ inteiros que servem de testemunhas. Se existe um testemunha a_i tal que N não satisfaz a congruência $a_i^{N-1} \equiv 1 \pmod{N}$ então N é composto. Se nenhum testemunha reconhecer N como sendo composto, isto é, se $a_j^{N-1} \equiv 1 \pmod{N}$ para $j = 1, 2, \cdots, k$, então, com uma forte probabilidade, N é primo.

O teste de RABIN é baseado na mesma idéia, os k números a_i testemunham se N satisfaz as congruências que definem os números fortemente pseudo-primos na base a_i. Neste teste, a conclusão é que N é composto ou N é primo com probabilidade $1 - \frac{1}{4^k}$; se k= 30, o teste é incorreto somente com um número entre 100 000 000 de números.

Evidentemente esses testes são muito fáceis de aplicar.

Agora, voltemos nossa atenção para os testes de primalidade que se aplicam aos números da forma $N \pm 1$, onde todos ou muitos dos fatores primos de N são conhecidos.

Os testes para os números $N + 1$ são baseados nas recíprocas fracas do pequeno teorema de FERMAT. Aqueles que se aplicam aos números $N - 1$ utilizam as seqüências de LUCAS.

Para os números de FERMAT $F_n = 2^{2^n} + 1$, PEPIN mostrou em 1877 que:

F_n é um número primo se e somente se

$$3^{(F_n-1)/2} \equiv -1 \pmod{F_n}.$$

A pesquisa da primalidade dos números F_n levou aos recordes seguintes:

RECORDE: F_4 é o maior número de FERMAT primo conhecido. O maior número de FERMAT do qual se conhece a fatoração em números primos é F_{11} (BRENT e MORAIN, 1988). O último (em data) número de FERMAT cuja fatoração em números primos já foi determinada é F_9 (A.K. LENSTRA e M. MANASSE, 1990).

F_{23471} é o maior número de FERMAT que se sabe ser composto; ele possui o fator $5 \times 2^{23473} + 1$ (W.KELLER, 1983).

F_{22} é o menor número de FERMAT do qual não se sabe se ele é primo ou composto.

Passemos agora aos números de MERSENNE $M_q = 2^q - 1$ (onde q é primo).

Para esses números aplica-se o teste de LUCAS (1878).

Seja $S_o = 4, S_{k+1} = S_k^2 - 2$ (para $k \geq 0$). Então M_q é um número primo se e somente se M_q divide S_{q-2} . Este teste permitiu descobrir números primos muito grandes.

RECORDE: Até o presente, são conhecidos 31 números de MERSENNE primos. O maior deles, descoberto por D. SLOWINSKI em 1985, é M_q com $q = 216091$. Este número tem 65050 algorítmos e evidentemente não se saberia testar a primalidade de um número assim tão grande se ele não fosse de uma forma especial.

O último (em data) número de MERSENNE reconhecido como primo foi M_q com $q = 110503$ (por W.N. COLQUIT e L. WELSCH JR., em 1988).

O maior número de MERSENNE composto conhecido é M_q com $q = 39051 \times 2^{6001} - 1$ (descoberto por W. KELLER, 1987).

Durante muito tempo (desde 1876, quando E. LUCAS mostrou que M_{127} é primo), o título de " maior número primo conhecido" foi sempre referido a um número de MERSENNE.

Mas isto não é verdade!

RECORDE: O maior número primo conhecido atualmente* é

$$391581 \times 2^{216193} - 1$$

*Já superado por $2^{756839} - 1$. (Veja Amer. Math. Monthly, vol. 99, nº4

Sua descoberta em 1989 é devido a seis matemáticos dos quais o primeiro em ordem anti-alfabética (por que não?) é S. ZARANTONELLO; os outros cinco são J. SMITH, G. SMITH, B. PARADY, L. C. NOLL. e J. BROWN.

4. A distribuição dos números primos.

Até o momento sabemos que:

1) Existe uma infinidade de números primos
2) Não existe fórmula razoavelmente simples para os números primos.
3) É possível reconhecer se um número não excessivamente grande é primo.

Mas o que pode ser dito sobre a maneira como os números primos se distribuem entre os números naturais? A propósito disto, eu menciono alguma coisa vaga após a demonstração de EULER sobre a existência de uma infinidade de números primos — eles formam um conjunto mais rarefeito que aqueles dos quadrados (por exemplo).

Uma idéia muito simples para abordar a distribuição dos números primos consiste em contar os números primos inferiores à um número dado. Para todo número real $x > 0$, designemos por

$$\pi(x) = \#\{p \text{ primo} \mid p \leq x\};$$

$\pi(x)$ é a *função que conta os números primos.* Estuda-se o comportamento de $\pi(x)$, que é muito irregular, comparando essa função com funções mais simples. Este estudo leva a resultados de natureza assintótica

Já na idade de 15 anos, por observação de tabelas de números primos, C.F. GAUSS sugeriu que

$$\pi(x) \sim \frac{x}{\log x},$$

isto é, o limite (quando x tende para o infinito) de $\frac{\pi(x)}{x/\log x}$ existe e é igual a 1.

(1992) p. 360 e nº7, p. 617.) Lembremos o leitor de que o presente trabalho do Professor Ribenboim foi-nos submetido em agosto de 1991. (N.E.)

Uma formulação equivalente é a seguinte:

$$\pi(x) \sim \int_1^x \frac{dt}{\log t}$$

(esta última função é a chamada a *integral logarítmica* e é denotada $Li(x)$)

A afirmação de GAUSS foi demonstrada por J. HADAMARD e C. DE LA VALLÉE POUSSIN, anteriormente P. L. TSCHEBYCHEFF havia mostrado que se o limite existe, ele é necessariamente igual a 1.

Pode-se dizer sem risco que se trata do teorema mais importante da teoria dos números primos — por esta razão é hábito chamá-lo *o teorema dos números primos.*

Evidentemente este teorema não diz nada sobre o valor exato de $\pi(x)$. A propósito disto, existe uma fórmula, devida à E.D.F. MEISSEL, célebre astrônomo, que forneceu, em 1871, o valor exato de $\pi(x)$ em termos dos valores $\pi(y)$ para todo $y \leq x^{2/3}$ e de números primos $p \leq x^{1/2}$.

RECORDE: O maior inteiro N para o qual $\pi(N)$ foi calculado exatamente é $N = 4 \times 10^{16}$. J. C. LAGARIAS, V. S. MILLER e A. ODLYZKO (1985) determinaram

$$\pi(4 \times 10^{16}) = 1.075.292.778.753.150.$$

As diferenças $|\pi(x) - \frac{x}{\log x}|$ e $|\pi(x) - Li(x)|$ não permanecem limitadas quando x tende para o infinito. O cálculo tão exato quanto possível desses termos de erros é essencial nas aplicações do teorema dos números primos.

Inicialmente foi sugerido pelas tabelas e em seguida foi demonstrado por J. B. ROSSER e L. SCHOENFELD, em 1962, que $\frac{x}{\log x} \leq \pi(x)$ para todo $x \geq 17$.

A história é mais interessante no que concerne à diferença $Li(x) - \pi(x)$; segundo J. E. LITTLEWOOD esta diferença muda de sinal uma infinidade de vezes.

RECORDE: Em 1955, S. SKEWES mostrou que a diferença $Li(x) - \pi(x)$ é negativa para um x_o tal que

$$x_o < e^{e^{e^{e^{7,7}}}}$$

O menor x_o conhecido tal que $Li(x_o) \leq \pi(x_o)$ é tal que $x_o \leq 669 \times 10^{370}$, como foi demonstrado por H. J. J. TE RIELE (1986).

Sem sombra de dúvida, a função mais importante no estudo da distribuição dos números primos é a *função zeta* de RIEMANN.

Para todo o número complexo s, tal que $Re(s) > 1$, a série

$$\sum_{n=1}^{\infty} \frac{1}{n^s}$$

é absolutamente convergente; ela é também uniformemente convergente em cada domínio $\{s \mid Re(s) > 1 + \epsilon\}$ (onde $\epsilon > 0$ é dado arbitrariamente). A função $\zeta(s)$ assim definida admite um prolongamento analítico a uma função meromorfa, definida sobre todo o plano complexo e tendo um só polo em $s = 1$, que é de ordem 1 com resíduo igual a 1. O estudo das propriedades dessa função permitiu, eventualmente, demonstrar o teorema dos números primos.

$\zeta(s)$ tem os zeros -2, -4, -6,$\cdots$ o que pode ser descoberto sem dificuldade pela equação funcional. Todos os outros zeros de $\zeta(s)$ são números complexos $\sigma + it$ (σ, t reais), com $0 < \sigma < 1$.

A hipótese de RIEMANN (que é de fato uma conjectura ainda não demonstrada) se enuncia:

Os zeros não triviais da função zeta de RIEMANN encontram-se sobre a *reta crítica* dos pontos $\frac{1}{2} + it$ (t real).

Sem entrar em detalhes, existem muitos teoremas sobre a distribuição dos números primos que podem ser demonstrados supondo-se a hipótese de RIEMANN. É portanto essencial determinar os zeros não triviais de $\zeta(s)$; por simetria, é suficiente considerar aqueles para os quais $t > 0$.

Pode-se enumerar esses zeros como segue: denota-se o n-ésimo termo por $\sigma_n + it_n$ de modo que $t_n \leq t_{n+1}$ e se $t_n = t_{n+1}$ então $\sigma_n < \sigma_{n+1}$ (é necessário observar que existe exatamente um número finito de zeros com um valor dado de t)

RECORDE: Para $n \leq 1.500.000.001$, os zeros $\sigma_n + it_n$ da função zeta de RIEMANN se encontram sobre a reta crítica, isto é $\sigma_n = \frac{1}{2}$. Estes cálculos foram feitos por J. J. H. TE RIELE, J. VAN DE LUNE e D. T. WINTER, até 1986.

Uma outra abordagem deste problema foi desenvolvida por N. LEVINSON.

RECORDE: B. CONREY mostrou em 1989 que pelo menos 2/5 dos zeros da função zeta de RIEMANN encontram-se sobre a reta crítica.

As considerações precedentes se referiam ao comportamento assintótico da função $\pi(x)$ e à função $\zeta(s)$ que é essencial para a estimativa do termo de erro. Pode-se dizer que se trata do comportamento de $\pi(x)$ "no infinito."

Abordemos agora o comportamento *local* de $\pi(x)$, ou seja, o estudo das lacunas entre números primos.

A questão principal é a seguinte:

Conhecendo-se o n-ésimo número primo p_n, onde se encontra o número primo seguinte?

Trata-se portanto do estudo da diferença

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

É facil mostrar que

$$\limsup d_n = \infty,$$

isto é, existem blocos de números compostos sucessivos arbitrariamente grandes. Por exemplo:

$$(N+1)!+2, (N+1)!+3, \cdots, (N+1)!+(N+1)$$

são (para todo N) números compostos.

O interessante é encontrar grandes blocos de números compostos sucessivos e pequenos.

RECORDE: Em 1989, J. YOUNG e A. POTLER encontraram a lacuna seguinte:

$$p_n = 90.874.329.411.493$$

com

$$d_n = 804$$

O que se pode dizer sobre o limite inferior da seqüência das diferenças d_n?

Dizemos que dois números primos $p < p'$ são *gêmeos* se $p' - p = 2$

Não se sabe se existe uma infinidade de números primos gêmeos. Ou, dito de outra forma: não se sabe se $\liminf d_n = 2$.

A questão é delicada. Em 1919, V. BRUN mostrou que:

$$\sum(\frac{1}{p} + \frac{1}{p+2}) = B < \infty$$

(soma para todos os pares de números primos gêmeos)

Portanto, se existe uma infinidade de números primos gêmeos (como se imagina), eles formam um conjunto bem disperso.

Em 1976, R.P. BRENT calculou a constante de BRUN com bastante rigor:

$$B = 1,90216054...$$

RECORDE: O maior par conhecido de números primos gêmeos foi descoberto em 1989 por B. K. PARADY, J. F. SMITH, S. ZARANTONELLO do grupo dos "SEIS" DE AMDAHL (os mesmos que detêm, até o momento, o recorde do maior número primo descoberto). É o par $1706595 \times 2^{11235} \pm 1$.

O interesse em determinar grandes lacunas entre números primos não muito grandes pode ser melhor detalhado. É necessário estudar a seqëncia $\frac{d_n}{p_n}$ que indica as lacunas relativas.

Já em 1845 J. BERTRAND tinha concluído, observando as tabelas, que sempre existe um número primo entre p_n e $2p_n$ (para todo $n \geq 1$). TSCHEBYCHEFF foi o primeiro a demonstrar este resultado, que também se escreve: $p_{n+1} < 2p_n$ ou ainda $\frac{d_n}{p_n} < 1$.

É um bonito resultado mas bem mais fraco do que se pode deduzir do teorema dos números primos:

$$\lim \frac{d_n}{p_n} = 0$$

A teoria das lacunas entre números primos levou à formulação da conjectura:

Para todo $\epsilon > 0$ tem-se $p_{n+1} < p_n^{\frac{1}{2}+\epsilon}$, para n suficientemente grande.

RECORDE: Prosseguindo na linha de numerosos predecessores, o recorde é detido, neste momento, por MOZZOCHI (1986):

$$p_{n+1} < p_n^{\frac{1}{2}+\frac{1}{20}-\frac{1}{384}}$$

para n suficientemente grande.

Preocupado em não tornar esta exposição excessivamente longa, sou obrigado a passar em silêncio sobre muitas questões de grande interesse. Assim, não direi nada sobre os números primos em progressão aritmética e nem sobre o problema de GOLDBACH. Felizmente, atualmente existe um livro onde esses fatos e muitos outros estão reunidos e explicados em detalhes. Este livro só espera ser lido!

Terminarei esta exposição com algumas curiosidades que poderão ser contadas aos seus amigos em um coquetel (mas não depois de vários copos!)

Um número que se escreve $Rn = 111\cdots1$ (n algarismos decimais iguais a 1) é uma *repunidade*.

Não é sabido se existe uma infinidade delas que sejam números primos.

RECORDE: H. C. WILLIAMS e H. DUBNER mostraram em 1986 que R1031 é um número primo. As únicas outras repunidades que se sabe serem números primos são

$$R2, R19, R23, R317.$$

Enfim, um recorde curioso:

RECORDE: O maior número primo conhecido cujos algarismos são todos números primos é

$$7532 \times \frac{10^{1104}-1}{10^4-1} + 1$$

Se você deseja saber porque e como encontrá-lo, será necessário perguntar a H. DUBNER, que afirmou isto em 1988.

5. Conclusão.

Os assuntos que pertencem às seções (V) e (VI) (números primos especiais e heurística e experimentação) não foram considerados nesta exposição.

Como já afirmei, estes e muitos outros fatos se encontram reunidos sob uma capa amarela.

A observação e o estudo dos números primos, sob o ângulo desta apresentação, se revela um método muito fecundo e sobretudo prazeiroso. Os matemáticos obtém muito prazer nesse estudo e isto vale a pena.

É preciso, como eu, pensar que os números são amigos..., amigos que nos dão problemas!

Bibliografia

1. Paulo Ribenboim, The Book of Prime Number Records (3ª edição), Springer-Verlag, New York, 1991.
2. Paulo Ribenboim, Selections du Livre des Records de Nombres Premiers, Presses Universitaires de France, Paris, 1991.

Department of Mathematics
Queen's University
Kingston, Ontario K7L 3N6,
Canada