O que vem à rede...

António Machiavelo
Departamento de Matemática Pura da Faculdade de Ciências da Universidade do Porto

A importância de ser ou não primo

Os números primos[1] têm sido objecto de encanto e mistério para sucessivas gerações de seres humanos desde, pelo menos, a Grécia antiga até aos nossos dias. A demonstração de que há uma infinidade de primos, contida na proposição 20 do livro IX dos *Elementos* de Euclides (ver: http://aleph0.clarku.edu/~djoyce/java/elements/elements.html)
é um monumento à elegância e ao engenho humano. Uma variação particularmente concisa dessa demonstração é[2]:

Para todo o número natural n>1, qualquer divisor primo de n!+1 é maior que n. Q.E.D.!


K. F. Glauss (1777-1855)

Um excelente "site" dedicado aos números primos é o *The Prime Pages*, mantido por Chris Caldwell desde 1994 em: http://www.utm.edu/research/primes.


J. Hadarmard (1865-1963)

Uma das causas do fascínio por estes números é sem dúvida o serem aparentemente "indomáveis": parecem ocorrer de um modo completamente caótico entre os números naturais, deixando a impressão de não haver nenhum padrão, nenhuma regularidade na forma como se sucedem. Mas apesar dessa aparente desorganização individual, os primos têm alguma ordem quando agrupados e "em média".


Vallée Poussin (1866-1962)

Neste aspecto, o resultado mais notável é sem dúvida o conjecturado por K. F. Gauss (1777—1855) mas só demonstrado cerca de cem anos depois por C. de la Vallée Poussin (1866—1962) e J. Hadarmard (1865—1963), independentemente um do outro, resultado esse que é conhecido como *O Teorema dos Números Primos*: o número de primos até x é assimptoticamente aproximado por $x/\log(x)$. Ver: http://www.utm.edu/research/primes/howmany.shtml.

Uma família de números primos que tem merecido, há já vários séculos, uma atenção especial é a dos números conhecidos pelo nome de *primos de Mersenne*: os números primos da forma[3] $M_p=2^p-1$, por causa da sua relação com os números perfeitos[4]. Para estes números há um teste de primalidade particularmente eficiente, o teste de Lucas-Lehmer (ver http://www.utm.edu/research/primes/prove/prove3_2.html),
que faz com que os maiores primos conhecidos sejam desta forma. Neste momento, e desde 15 de Maio de 2004, o maior primo conhecido é $M_{24\,036\,583}$, um número com 7 235 733 algarismos! Este é mais um recorde do projecto *GIMPS*, *the Great Internet Mersenne Prime Search*, no qual o leitor poderá colaborar, como está explicado em: http://www.mersenne.org/prime.htm.

Como é que se sabe que tem 7 235 733 dígitos? Certamente que ninguém os contou um a um! O que se faz é usar a seguinte observação muito simples: como 10^{n-1} é o primeiro número com n dígitos, resulta que N tem n dígitos se e só se $10^{n-1} \leq N < 10^n$, o que é equivalente a $n-1 \leq \log_{10}(N) < n$. Daqui se conclui que: o número de dígitos de N é igual a $\lfloor \log_{10}(N) \rfloor + 1$, onde $\lfloor x \rfloor$ denota a *parte inteira* de x, isto é o maior inteiro que não ultrapassa x. O leitor poderá agora facilmente verificar,

numa simples calculadora, que $M_{24\ 036\ 583}$ tem de facto o número de algarismos referido.

Como se pode deduzir da consulta das páginas acima mencionadas, são dispendidos grandes recursos computacionais e humanos na procura de primos gigantes. Porquê? Algumas respostas são dadas em http://www.utm.edu/research/primes/notes/faq/why.html.

No fundo é apenas mais uma instância daquilo que nos define como humanos: a curiosidade de conhecer, de conhecer os limites da nossa espécie, e de tentar transcender esses mesmos limites. As vantagens evolutivas desta atitude deviam ser óbvias!

Nos últimos 30 anos o problema de distinguir números primos de números compostos, e o de factorizar estes últimos, ganhou toda uma outra importância devido ao advento da criptografia de chave pública. De tal modo que há quem ofereça prémios que vão desde US $20 000 até US $200 000 pela factorização de certos números! Ver: http://www.rsasecurity.com/rsalabs/node.asp?id=2093.

Há várias conjecturas famosas sobre números primos (ver http://www.utm.edu/research/primes/notes/conjectures), das quais se destacam:

- a *conjectura de Goldbach*: http://www.informatik.uni-giessen.de/staff/richstein/ca/Goldbach.html e http://www.ieeta.pt/~tos/goldbach.html.
- a *Hipótese de Riemann*, que é agora um dos "problemas do milénio": http://www.claymath.org/millennium e http://www.utm.edu/research/primes/notes/rh.html.

Recentemente resolveram-se duas velhas questões sobre números primos: foi encontrado um algoritmo de primalidade que é "polinomial" (o tempo que o algoritmo demora é majorado por uma função polinomial no tamanho do "input"), em Agosto de 2002. Ver: http://www.cse.iitk.ac.in/news/primality.html. e http://www.ams.org/notices/200305/fea-bornemann.pdf.

Em Abril deste ano, Ben Green e Terence Tao, terão provado a existência de progressões aritméticas arbitrariamente longas de números primos. O respectivo trabalho, ainda não publicado e em fase de revisão, pode ser consultado em: http://front.math.ucdavis.edu/math.NT/0404188.

Estes são dois avanços espectaculares que colocam, desde já, este início do século XXI como um momento importante na já longa história da tentativa do *Homo Sapiens* decifrar os recônditos mistérios dos números primos!

Os primeiros 100 primos

2, 3, 5, 7,	11, 13, 17,	19, 23, 29,	31, 37, 41,
43, 47, 53,	59, 61, 67,	71, 73, 79,	83, 89, 97,
101, 103,	107, 109,	113, 127,	131, 137,
139, 149,	151, 157,	163, 167,	173, 179,
181, 191,	193, 197,	199, 211,	223, 227,
229, 233,	239, 241,	251, 257,	263, 269,
271, 277,	281, 283,	293, 307,	311, 313,
317, 331,	337, 347,	349, 353,	359, 367,
373, 379,	383, 389,	397, 401,	409, 419,
421, 431,	433, 439,	443, 449,	457, 461,
463, 467,	479, 487,	491, 499,	503, 509,
521, 523,	541, ...		

[1] Números naturais, maiores que a unidade, que não podem ser escritos como produto de números menores.

[2] Para benefício dos leitores que nunca viram este argumento, observe-se que se usam aqui dois factos simples sobre os números naturais: 1) Todo o número natural maior que um tem algum divisor primo, pois ou já é primo ou então tem um divisor menor que ele e ainda maior que um, que por sua vez ou é primo ou ...etc..., e como só há um número finito de números menores que um dado número, este "etc" tem de terminar com um divisor primo do número inicialmente dado; 2) Se o número natural m for múltiplo de um número natural maior que um, então $m+1$ não o é. Portanto, dado um qualquer número natural $n>1$, por (1) existe um primo que divide $n!+1$, e por (2) este primo não pode ser nenhum dos números 2, 3, ..., n. Isto mostra que dado um número qualquer n, há sempre um primo que é maior que n, de onde resulta que o conjunto dos números primos é infinito.

[3] Não é difícil ver que 2^n-1 só pode ser primo se n o for (mas não o recíproco!).

[4] Um número diz-se *perfeito* se igualar a soma dos seus divisores, incluindo 1 mas excluindo o próprio; os primeiros quatro números perfeitos são 6, 28, 496 e 8128. Os *Elementos* de Euclides contêm a observação que se p for tal que 2^p-1 é um número primo, então o número $2^{p-1}(2^p-1)$ é perfeito. Cerca de 2000 anos depois dos *Elementos* terem sido escritos, Euler demonstrou que estes são os únicos números perfeitos pares. A existência ou não de um número perfeito ímpar é o problema de Matemática mais antigo ainda em aberto.