por António Machiavelo
[Departamento de Matemática da Faculdade de Ciências da Universidade do Porto]

Números de Fermat

Fermat suspeitava de que os números da forma $2^{2^n}+1$ seriam todos primos. Estava errado (algo raro em Fermat), mas este erro não deixou de criar um desafio que, ainda hoje, dá muito que fazer: o de factorizar estes números, que são, em muitos aspectos, realmente singulares. E este ano de 2010 conta já com alguns avanços históricos na procura dos factores destes números.

Numa carta dirigida a Frénicle de Bessy (c. 1605-1675), muito possivelmente escrita em Agosto de 1640, da qual é conhecido apenas um fragmento, o juiz conselheiro do parlamento de Toulouse e matemático nas horas livres Pierre de Fermat (1601 ou 1607/8-1665)[1] escreveu:

[...] estou quase persuadido de que todos os números [da forma $2^{2^n}+1 (n \in \mathbb{N}_0)$][2] *são números primos...*

Não tenho uma demonstração exacta disto, mas excluí uma tão grande quantidade de divisores através de demonstrações infalíveis, e tenho umas tão grandes luzes que fundamentam o meu pensamento, que teria dificuldade em me desdizer.

Fermat repetiria esta sua convicção em várias outras cartas[3] ao longo da vida. O interesse num resultado deste tipo seria o de poder dar-se exemplo, de um modo relativamente fácil, de números primos tão grandes quanto se queira, o que ainda hoje não se sabe fazer. Isto apesar de, em 1964, C. P. Willans ter construído[4] uma fórmula para o n-ésimo número primo, P_n, a partir do teorema de Wilson[5] que caracteriza os números primos como os números k tais

Retrato de Fermat, por Roland Lefèvre (Musée de la Ville de Narbonne)

[1] Há algumas dúvidas sobre a data de nascimento de Fermat: ver *http://www.emis.de/newsletter/newsletter42.pdf*, p. 12.
[2] Fermat diz isto de um outro modo, que não interessa aqui referir. Ver pp. 205-206 do segundo volume das *Oeuvres de Fermat*, publicadas por Paul Tannery e Charles Henry, Gauthier-Villars (1891-1912), disponíveis em *http://quod.lib.umich.edu/u/umhistmath*. Relembre-se que 2^{2^n} representa, por convenção (para evitar o uso de alguns parêntesis), o número $2^{(2^n)}$, e não $(2^2)^n$.
[3] De novo a Frénicle, em 18 de Outubro de 1640 (pp. 207-208 do vol. II das *Oeuvres de Fermat*), a Mersenne em 25 de Dezembro de 1640 (pp. 212-213), a Pascal em 29 de Agosto de 1654 (p. 309-310), a Kenelm Digby em Junho de 1658 (pp. 404-405; p. 316 do vol. III), a Carcavi em Agosto de 1659 (p. 434).
[4] C. P. Willans, "*On Formulae for the nth Prime Number*", *The Mathematical Gazette* **48** (1964) 413-415.
[5] Apesar de ter este nome, este resultado era já conhecido por Bhaskara (séc. VII) e, posteriormente, por al-Haytham (séc. X-XI). John Wilson (1741-1793) apenas o redescobriu, não o tendo conseguido demonstrar. A primeira demonstração conhecida do teorema "de Wilson" foi dada por Lagrange, em 1773 (*http://en.wikipedia.org/wiki/Wilson's_theorem*).

Caderno_2
quarta-feira, 23 de Junho de 2010 14:07:19

que $\frac{(k-1)!+1}{k}$ é um número inteiro:

$$P_n = 1 + \sum_{m=1}^{2^n} \left\lfloor \left(\frac{1}{n} \sum_{k=1}^{m} \left\lfloor \cos^2 \pi \frac{(k-1)!+1}{k} \right\rfloor \right)^{-1/n} \right\rfloor$$

onde (x) denota a parte inteira de x, ou seja, o maior inteiro que não ultrapassa x. Várias outras fórmulas foram entretanto construídas[6], em geral de alguma forma codificando um ou outro critério de primalidade, mas são todas computacionalmente inúteis, não permitindo calcular efectivamente números primos "grandes", não se conhecendo nenhuma expressão que, dado um número natural n, forneça um número primo tanto maior quanto n o for e que dê lugar a um número de operações simples[7] que seja directamente proporcional a n. A expressão de Fermat, $2^{2^n}+1$, daria uma tal função.

Mas o arquitecto da Teoria dos Números moderna estava errado, e os números $F_n=2^{2^n}+1$, hoje conhecidos como *números de Fermat*, não são todos primos. De facto, em 1732, Euler mostra que 641 divide F_5, algo que Fermat poderia ter facilmente feito se não estivesse, por razões que se desconhecem, tão convencido de que eram todos primos. Sabe-se hoje que F_n é composto para $n \in \{5, 6, ..., 32\}$. O número F_{33}, um gigante com 2 585 827 973 algarismos (!), é assim o primeiro número de Fermat que não se sabe se é primo ou composto. Wilfrid Keller da Universidade de Hamburgo mantém uma página com as últimas informações sobre a factorização destes números em:

http://www.prothsearch.net/fermat.html

A primalidade de um número de Fermat pode ser decidida com uma única divisão, em consequência de um resultado publicado em 1877 por Jean François Pépin (1826-1904):

F_n é primo se e só se F_n dividir $3^{\frac{F_n-1}{2}}+1$,

hoje conhecido como *teste de Pépin*[8]. Essa divisão pode ser efectuada muito eficientemente usando bons algoritmos de exponenciação modular[9]. O grande obstáculo à determinação da primalidade dos números de Fermat é o crescimento desmesurado destes, cujo número de algarismos, grosso modo, duplica quando se passa de um deles para o seguinte. Isto faz com que seja um autêntico desafio lidar com estes números.

Mas mais complicado ainda é encontrar um divisor próprio de um número de Fermat[10], mesmo depois de se saber que este é composto. No início deste ano de 2010 sabia-se, graças ao teste de Pépin, de quatro números de Fermat que eram compostos, sem se conhecer nenhum dos seus factores: F_{14}, F_{20}, F_{22}, F_{24}, (desde 1963, 1987, 1993 e 1999, respectivamente). Causou, pois, alguma sensação o anúncio, a 3 de Fevereiro, de que tinha sido encontrado um factor primo de F_{14} (4933 algarismos):

$$17841809978191279575963744176421565451108810947 17\times 2^{16}+1.$$

Veja-se a reacção entusiástica dos respectivos *tifosi*, em:

http://www.mersenneforum.org/showthread.php?=13051

Para adicionar à festa, a 26 de Março, foi anunciada a descoberta de um factor de F_{22} (1 262 612 algarismos!): $38535920244406765753363221 1\times 2^{24}+1$. E no dia seguinte, a 27 de Março, foi encontrado o sexto factor primo de F_{12}, que, apesar disso, não está ainda completamente factorizado! Como pode ser visto no início da página de W. Keller acima mencionada, e respectivos *links*, os adeptos estão ao rubro! Como alguém já declarou no fórum *www.mersenneforum.org*: "Este é o ano em que se fez contacto com muitos factores de Fermat!"

As atenções estão agora centradas em F_{20}, F_{24}, e F_{33}. Para ajudar na busca, o leitor interessado em colaborar na procura distribuída dos factores dos números de Fermat deve ir a

http://www.fermatsearch.org

Quem sabe se não acaba o ano a brindar com a equipa! Boa sorte!

[6]Ver *http://en.wikipedia.org/wiki/Formula_for_primes* e *http://mathworld.wolfram.com/PrimeFormulas.html*.
[7]Para as quais exista um programa que as execute com um número de passos directamente proporcional ao tamanho do maior dos dados de entrada (i.e. do *input*).
[8]Ver *http://primes.utm.edu/prove/prove3_1.html*
[9]Ver *http://en.wikipedia.org/wiki/Exponentiation_by_squaring*
[10]Sabe-se que um factor primo de F_n tem deter a forma $2^{n+2}k + 1$.

Caderno_2
quarta-feira, 23 de Junho de 2010 14:07:23