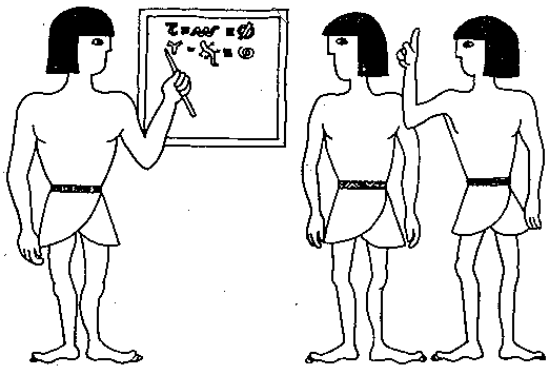
Histórias e histórias...

Números de Fermat

Paulo Ferreira Leite
IME–USP
Cx. P. 20570
01498 – São Paulo – SP



A primeira e mais fundamental pergunta sobre números primos foi respondida por Euclides, há mais de dois mil anos, ao provar que esses números formam um conjunto infinito.

Motivados por esse resultado muitos matemáticos tentaram encontrar fórmulas que fornecessem, senão todos, pelo menos, uma infinidade de primos.

Fermat (Pierre de Fermat: 1601-1658), um dos maiores matemáticos do século XVII, acreditava conhecer uma tal fórmula. Em carta endereçada a seu amigo Bernard Frenide de Bessy datada de provavelmente agosto de 1640 revelava ele, embora confessando não estar de posse de uma prova completa, sua convicção de que os números $F_n = 2^{2^n}+1$ eram primos para todos os valores do natural n.

$$F_0 = 2^{2^0}+1 = 3,\ F_1 = 2^{2^1}+1 = 5,$$

$$F_2 = 2^{2^2}+1 = 17,\ F_3 = 2^{2^3}+1 = 257$$

$$\text{e } F_4 = 2^{2^4}+1 = 65537$$

são efetivamente primos: $F_5 = 2^{2^5}+1 = 4.294.967.297$ já é suficientemente grande para ter impedido que Fermat se certificasse de sua natureza e $F_6 = 2^{2^6}+1 = 18.446.744.073.709.551.617$ é um número bastante grande, mesmo para os padrões de hoje, quando dispomos de computadores.

Apesar de ciente de não possuir uma demonstração, Fermat voltou, em várias outras ocasiões, inclusive em carta endereçada a Pascal em 1654, a reiterar sua crença na primalidade desses números.

O problema, no entanto, só ficou definitivamente resolvido quando Euler, em 1732, provou, mostrando que 641 é um fator de F_5, ser a conjectura falsa. A partir daí, por uma ironia do destino, em todos os casos em que foi possível decidir, os números F_n se revelaram compostos. (veja quadro 1). Não obstante, uma conjectura de Eisenstein afirmando que existem infinitos primos da forma $2^{2^n}+1$ permanece em aberto.

O resultado que talvez mais tenha contribuído para que os números de Fermat adquirissem uma certa notoriedade foi a descoberta por Gauss em 1796, de que uma circunferência pode ser dividida (com régua e compasso) em n partes iguais, se e somente se $n = 2^m p_1 p_2 \ldots p_k$ onde m é um natural e $p_1, p_2, \ldots, p_k$ são primos de Fermat distintos(*).

Uma outra propriedade interessante dos números de Fermat, da qual decorre uma demonstração diferente da de Euclides de que existem infinitos primos, é que eles formam uma seqüência infinita de números

(*) Para maiores detalhes veja RPM, nº 4, páginas 1-3.

QUADRO 1

Fatores de F_n, $5 \leq n \leq 22$

n	Fatores Primos	Data	Descoberto por
5	641	1729	EULER
5	6700417	1729	EULER
6	274177	1880	LANDRY
6	67280421310721	1880	LANDRY, LeLASSEUR, GERARDIN
7	59649589127497217	1970	MORRISON, BRILLHART
7	5704689200685129054721	1970	MORRISON, BRILLHART
8	c	1909	MOREHEAD, WESTERN
9	2424833	1903	WESTERN
9	c	1967	BRILLHART
10	45592577	1953	SELFRIDGE
10	6487031809	1962	BRILLHART
10	c	1967	BRILLHART
11	319489	1899	CUNNINGHAM
11	974849	1899	CUNNINGHAM
12	114689	1877	LUCAS, PERVOUCHINE
12	26017793	1903	WESTERN
12	63766529	1903	WESTERN
12	190274191361	1974	HALLYBURTON, BRILLHART
13	2710954639361	1974	HALLYBURTON, BRILLHART
14	c	1961	SELFRIDGE, HURWITZ
15	1214251009	1925	KRAITCHIK
16	825753601	1953	SELFRIDGE
17	?		
18	13631489	1903	WESTERN
19	70525124609	1962	RIESEL
19	646730219521	1963	WRATHALL
20	?		
21	4485296422913	1963	WRATHALL
22	?		

? = Não se sabe se F_n é, ou não, primo

c = F_n é composto

dois a dois primos entre si, isto é, se $m \neq n$ então $m.d.c(F_m, F_n) = 1$. De fato, admitindo-se que eles são dois a dois primos entre si, a demonstração de que existem infinitos primos decorre da observação de que a cada termo F_n da seqüência está associado pelo menos um divisor primo diferente dos divisores primos associados aos termos anteriores da seqüência.

Muito embora pudéssemos mencionar várias outras propriedades da seqüência F_n, algumas teoremas, outras, meras conjecturas, preferimos terminar examinando um outro tipo de questão: o que teria levado Fermat a supor serem os números $F_n = 2^{2^n} + 1$ todos eles primos?

Essa é uma questão intrigante e de difícil resposta. A explicação mais corrente de que a conjectura foi feita por indução vulgar, levando em conta apenas o fato de que os cinco primeiros números da seqüência são primos, não pode ser aceita sem restrições por não ser esse um erro que se deva esperar de um matemático do porte de Fermat.

Uma outra explicação, talvez mais convincente, foi proposta pelo astrônomo polonês Banachiewicz [3]. Sugeriu ele que Fermat pode ter provado (o que é realmente verdadeiro) que F_n divide $2^{F_n} - 2$ reduzindo assim a prova da primalidade de F_n a um suposto teste de primalidade que os matemáticos chineses da antigüidade acreditavam ser verdadeiro e que, até a época de Fermat, permanecia em aberto, isto é, não se sabia

QUADRO 2

F_n divide $2^{F_n} - 2$

Na prova deste fato, usaremos o conceito e algumas propriedades das congruências:

Congruências

Sejam a, b e m > 0 números inteiros.
Dizemos que a e b são congruentes módulo m se m divide b – a.
Em símbolos

$$a \equiv b \mod m^{(*)}$$

Utilizaremos as seguintes propriedades das congruências:

$$\begin{cases} a \equiv b \\ e \\ c \equiv d \end{cases} \mod m \rightarrow \begin{cases} a + c \equiv b + d \\ e \\ ac \equiv bd \end{cases} \mod m$$

Em particular

$a \equiv b \mod m \rightarrow ac \equiv bc \mod m$
$a \equiv b \mod m \rightarrow a^n \equiv b^n \mod m,\ n > 0$

Prova

É claro que $2^{2^n} + 1 \equiv 0 \mod F_n \therefore 2^{2^n} \equiv -1 \mod F_n$

$\therefore (2^{2^n})^{2(2^n - n)} \equiv (-1)^{2(2^n - n)} \mod F_n$

$\therefore 2^{2^{2^n}} \equiv 1 \mod F_n$.

$2 \times 2^{2^{2^n}} \equiv 2 \mod F_n$.

$2^{2^{2^n}+1} \equiv 2 \mod F_n$.

$2^{F_n} \equiv 2 \mod F_n$.

$F_n \mid 2^{F_n} - 2$

(*) Essa notação foi introduzida por Gauss, que foi também o primeiro matemático a usar de forma sistemática a noção de congruência, em seu livro Disquisitiones Arithmeticae, publicado em 1801.

se era verdadeiro ou falso. Mais precisamente, o teste afirmava que uma condição necessária e suficiente para que um inteiro $n \geqslant 2$ fosse primo era que n dividisse $2^n - 2$. A condição é realmente necessária e o próprio Fermat, demonstrou um resultado mais geral: se a é um inteiro positivo e p um primo então p divide $a^p - a$. É possível que Fermat acreditasse que a condição fosse também suficiente bastando portanto que tivesse provado ser F_n um divisor de $2^{F_n} - 2$ para concluir que estava diante de um primo. Sua alegação de não estar de posse de uma demonstração poderia, nesse caso, referir-se ao fato de não saber demonstrar a suficiência (que não é mesmo verdadeira) do teste chinês.

O primeiro contra-exemplo explícito para o teste foi, no entanto, dado somente em 1819 por Sarrus ao provar que $341 = 11 \times 31$ divide $2^{341} - 2$. Vale a pena, porém, observar que, admitindo-se conhecido o fato de que F_n divide $2^{F_n} - 2$, verificamos que Euler, ao provar em 1732 que F_5 era composto, estava, na realidade, antecipando em 87 anos o contra-exemplo dado por Sarrus!

Bibliografia

[1] BOYER, Carl B. – *História da Matemática* (tradução Elza Furtado Gomide) Editora Edgard Blucher Ltda./Editora Universidade de São Paulo.

[2] KLINE, Morris – *Mathematical Thought from Ancient to Modern Times*, Oxford University Press.

[3] STARK, Harold M. – *An Introduction to Number Theory*, Oxford University Press.