

## Fermat number record established in Ireland

A mathematically significant number of supra-astronomical size was recently discovered in St. Patrick's College, Drumcondra. One of its two discoverers – Dr. John Cosgrave – explains.

Pierre de Fermat (1601-1665), the outstanding French mathematician, has gained public recognition following the solution by Andrew Wiles of the famous problem of Fermat's 'Last Theorem.' Recounted in a widely acclaimed BBC Horizon programme, the related book by Simon Singh entered the best-sellers list.

Today there remains only one unresolved question of Fermat's, one of such *apparent* simplicity that on first hearing of it you might be tempted to exclaim: I can solve that! However the consensus amongst mathematicians who have occupied themselves with this problem is that it may remain forever unresolved.

Fermat's question is, *what is the status of the 'Fermat numbers'?*, the Fermat numbers –  $F_0, F_1, F_2, F_3, \dots$  – being the unending sequence of numbers:

$$3, 5, 17, 257, 65537, 4294967297, 18446744073709551617, \dots$$

These numbers – formulated by Fermat in August 1640 – are formed in this simple way:

- starting from 2, a succession of numbers is formed by repeatedly squaring the previous one, producing: 2, 4, 16, 256, 65536, 4294967296, 18446744073709551616, ...
- add 1 to each, forming: 3, 5, 17, 257, 65537, 4294967297, 18446744073709551617, ...

The  $n^{\text{th}}$  Fermat number –  $F_n$  – is given by  $F_n = 2^{2^n} + 1$ , with  $n = 0, 1, 2, 3, 4, 5, \dots$ . For example,  $F_3 = 2^{2^3} + 1 = 2^8 + 1 = 257$ . Fermat believed *every*  $F$ -number to be prime (evenly divisible only by 1 and itself), but failed to prove it.

In 1732 the renowned Euler established that  $F_5 = 2^{2^5} + 1 = 2^{32} + 1 = 4294967297 = 641 \times 6700417$ , is evenly divisible by 641 and 6700417, establishing  $F_5$  as the smallest *composite* (not prime) Fermat number. In the intervening years no other Fermat number has been identified as being prime, and there is now a general belief (not shared by the writer) that *every* Fermat number from  $F_5$  onwards is composite.

$F_5$  to  $F_{23}$  are composite, but  $F_{24}$  (5,050,446 decimal digits), requiring a 47 by 47 feet surface to write it, allowing 4 digits per inch, is unresolved. A team led by Dr. Richard Crandall, has been attempting to establish its status (prime/composite?) for some time.

While  $F_{24}$  is large, it is insignificant compared to  $F_{382447}$ , found on July 24<sup>th</sup> in St. Patrick's College, Drumcondra, to be evenly divisible by  $3 \times 2^{382449} + 1$  (115130 digits). This almost unimaginably large number –  $F_{382447}$  (over  $10^{115136}$  digits) – would require a board measuring more than  $10^{57550}$  by  $10^{57550}$  *light years* to write it down, at 4 digits per inch, and even at  $10^{30}$  digits per inch, the requisite board would measure at least  $10^{57520}$  by  $10^{57520}$  light years.

How has this result (a new world record for a Fermat composite, surpassing Jeffrey Young's  $F_{303088}$ , found at Silicon Graphics) been established? It has been made possible by two French contributions: a beautiful idea (1878) due to a self-taught farmer, François Proth (1852-79), together with the brilliant computer program (*Proth.exe*) of a contemporary scientist, Yves Gallot, who lives – by a lovely twist of fate – in Toulouse, where Fermat conceived the numbers now bearing his name.

A public lecture entitled 'The history of Fermat numbers from August 1640' – using **Maple** software, and demonstrating Gallot's program – will be given by the writer in St. Patrick's later this year; details will be available from his web site <[www.spd.dcu.ie/johnbcos](http://www.spd.dcu.ie/johnbcos)>. That site gives links to Gallot's program, to the dedicated compilation work of Dr. Ray Ballinger of Florida University and Dr. Wilfrid Keller of Hamburg University, to the writer's 3<sup>rd</sup> year undergraduate notes on Proth's 1878 theorem, and to much else besides.