END ZONE

NUMBERS COUNT

Mike Mudge delves into the factorisation and other properties of Fermat Numbers, with mathematical requirements being kept to the minimum.

Definition 'Fermat Numbers' are defined by $F_n = 2^{2^n} + 1$. Thus, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$.

It can be readily verified that these first four Fermat Numbers are prime; indeed, Pierre De Fermat (1601-1665) conjectured that *all* F_n were prime. However, such are the dangers of generalisation based upon empirical evidence, and in 1732 Leonhard Euler found that:

$F_5 = 2^{2^5} + 1 = 2^{32} + 1 = 4294967297$
$= 641 \times 6700417$

In 1880 F Landry proved that:

$F_6 = 2^{2^6} = 2^{64} + 1 = 274177$
$\times 67280421310721$

No prime Fermat Number has been found beyond F_4, so that Fermat's conjecture has not proved to be a very happy one. It is perhaps more probable that although the number of prime F_n is finite, there are others waiting to be discovered (reference the probabalistic argument given as a footnote in *An Introduction to the Theory of Numbers* by GH Hardy and EM Wright).

The existence of prime F_n has an interesting geometrical connection, since Karl Friedrich Gauss proved that a regular polygon having F_n-sides could be inscribed in a circle by Euclidean methods if F_n is prime. (A 65537-sided regular polygon inscribed in a given circle could provide an interesting challenge in computer graphics, particularly if an attempt was made to simulate the Euclidean methods mentioned above!)

Theorem 1 No two Fermat Numbers have a common divisor other than 1.

Theorem 2 If F_n is prime, then the number:

$$Z_n = 3^{2^{2^n - 1}+1}$$

is divisible by F_n.

For example, $F_2 = 17$ is prime, hence we know that $3^{23} + 1 = 3^8 = 65\,61 + 1$ is divisible by 17. In fact, $6562 = 17 \times 386$.

Note The converse of theorem 2 is also true: that is, if F_n is *not* prime, then Z_n is *not* divisible by F_n.

Theorem 3 Any factor of F_n has the form $k \times 2^m + 1$ where $m \geq n + 2$ and k is an odd integer.

For example, the factor 274177 of F_6 cited above is given by $256 \times 1071 + 1$, while the factor 6700417 of F_5 is given by $52347 \times 128 + 1$.

This month's project is to search for factors of Fermat Numbers; it is suggested that Theorem 3 be used, hence two different ways of organising the search are possible.

The description which follows is due to Professor Wilfrid Keller of the University of Hamburg, who has conducted extensive research in this area using both a Telefunken TR 440 computer in TAS assembly language and a Siemens 7.755 with built-in extended precision floating point arithmetic.

How far can *PCW* readers get with this work?

Approach 1 — Trial division For fixed n, look for all k less than some search limit L_n to see if $k \times 2^{n+2} + 1$ divides some F_r, $r \leq n$.

Approach 2 — Tabulation of primes For fixed k, list all primes of the form $k \times 2^m + 1$ for m up to some limit M_k. Then, for each prime, look to see if it divides some F_n where $n \leq m - 2$.

Readers are invited to send their thoughts, together with attempts at this project, to Mike Mudge, 'Square Acre', Stourbridge Road, Penn, Staffordshire WV4 5NF, tel: (0902) 892141, to arrive by 1 December 1987.

It would be appreciated if such submissions contained a brief summary of results obtained, in a form suitable for publication in *PCW*. These submissions will be judged using subjective criteria, and a prize will be awarded by *PCW* to the 'best' contribution received by the closing date.

Please note that submissions can only be returned if a stamped addressed envelope is provided.

Belated review: September 1986

Regular readers of Numbers Count will be aware that the prize award associated with this problem was deferred (*PCW*, March) due to a lack of response. Interesting correspondence has since been generated, resulting in a very worthy prizewinner: Fred Hartley of 46 Hughes Road, Hayes, Middlesex UB3 3AP. Fred used a BBC Model B and relied very much upon a set of long integer arithmetic routines written in assembler which cope with integers up to 256 bytes in length.

The computing went hand in hand with a careful theoretical analysis, and Fred's third communication concludes: 'I suspect that s(k)/k increases without limit as the number of factors increases, but I have not proved this.' Can any mathematicians help?

I am certain that Fred would welcome enquiries from interested readers regarding the details of his work.

Review: March 1987

This problem was, as expected, extremely popular. It was prompted by the following results quoted in LE Dickson, *History of the Theory of Numbers, Volume 2.*

'Fermat noted that if in (205769, 190281, 78320) we add the area to the square of the sum of the legs, we get a square.

'Frenicle stated that in (17, 144, 145) the sum of the area and the hypotenuse is a square, while the first three right triangles in which the sum of the area and smaller leg is a square, are (3, 4, 5); (16, 30, 34) & (105, 208, 233).

'"Calculator" found three right triangles of equal perimeter and areas in arithmetical progression (18601944, 13951458, 23252430); (18559223, 13999464, 23247145) & (18515584, 14048388, 23241860)'.

While AH Beiler, *Recreations in the Theory of Numbers,* reports:

'Four primitive Pythagorean triangles having a common perimeter have also been found. Only seven such quadruples exist for a perimeter less than 1000000 so they are quite rare. The smallest of these perimeters is 317460 and the triangles are (153868, 9435, 154157); (99660, 86099, 131701); (43660, 133419, 140381) and (13260, 151811, 152389). Can the reader find the other six?'

Unfortunately, the italics in part (v) of the problem together with the lack of the adjective 'primitive' generated a great deal of computer output — at least one complete answer to that part!

After much consideration, this month's prizewinner is Peter Hicks of 9 Carramar Street, Rye, Victoria, 3941, Australia.

Mike Mudge welcomes correspondence on any subject within the areas of number theory and other computational mathematics. Particularly welcome are suggestions, either general or particular, for future Numbers Count articles; all letters will be answered in due course.

Isolated readers can be put into contact with others sharing the same interests. However, greater efficiency regarding published problems should result from contacting the prizewinner directly.