Problem 28: Fermat numbers (✓✓)

The nth Fermat number, F_n, is defined by

$$F_n = 2^{2^n} + 1\,, \qquad n = 0,\ 1,\ 2,\ \ldots\ ,$$

where 2^{2^n} means 2 raised to the power 2^n. Calculate F_0, F_1, F_2 and F_3. Show that, for $k = 1$, $k = 2$ and $k = 3$,

$$F_0 F_1 \ldots F_{k-1} = F_k - 2\,. \qquad (*)$$

Prove, by induction, or otherwise, that $(*)$ holds for all $k \geqslant 1$. Deduce that no two Fermat numbers have a common factor greater than 1.
Hence show that there are infinitely many prime numbers.

2002 Paper II

Comments

Fermat (1601–1665) conjectured that every number of the form $2^{2^n} + 1$ is a prime number. F_0 to F_4 are indeed prime, but Euler showed in 1732 that F_5 (4294967297) is divisible by 641. As can be seen, Fermat numbers get very big and not many more have been investigated; but those that have been investigated have been found not to be prime numbers. It is now conjectured that in fact only a finite number of Fermat numbers are prime numbers.

The Fermat numbers have a geometrical significance as well: Gauss proved that a regular polygon of n sides can be inscribed in a circle using a Euclidean construction (i.e. only a straight edge and a compass) if and only if n is a power of 2 times a product of distinct Fermat primes.

The very last part of this question, showing that the number of primes is infinite, is completely unexpected and delightful. It comes from *Proofs from THE BOOK*[20], a set of proofs thought by Paul Erdös to be heaven-sent. Most of them are much less elementary this one. Erdös was an extraordinarily prolific mathematician. He had almost no personal belongings and no home[21]. He spent his life visiting other mathematicians and proving theorems with them. He collaborated with so many people that every mathematician is (jokingly) assigned an *Erdös number*; for example, if you wrote a paper with someone who wrote a paper with Erdös, you are given the Erdös number 2. Most mathematicians seem to have an Erdös number less than 8.

[20] M. Aigler and G.M. Ziegler (Springer, 1999). The idea behind the proof was given by Christian Goldbach (1690–1764), who is best known for his conjecture that there are an infinite number of *twin primes*, that is, prime numbers that are two apart such as 17 and 19.

[21] See *The Man Who Loved Only Numbers* by Paul Hoffman, published by Little Brown and Company in 1999 — a wonderfully readable and interesting book.

Solution to problem 28

To begin with, we have by direct calculation that $F_0 = 3$, $F_1 = 5$, $F_2 = 17$ and $F_3 = 257$, so it is easy to verify $(*)$ for $k = 1, 2$ and 3.

For the induction, we start by assuming that the result holds for $k = m$ so that

$$F_0 F_1 \dots F_{m-1} = F_m - 2 \, .$$

We need to show that this implies that the result holds for $k = m + 1$, i.e. that

$$F_0 F_1 \dots F_m = F_{m+1} - 2 \, . \qquad (*)$$

Starting with the left-hand side of this equation, we have

$$F_0 F_1 \dots F_{m-1} F_m = (F_m - 2)F_m = (2^{2^m} - 1)(2^{2^m} + 1) = \left(2^{2^m}\right)^2 - 1 = 2^{2^{m+1}} - 1 = F_{m+1} - 2,$$

as required. Since we know that the result holds for $k = 1$, the induction is complete.

To show that no two Fermat number have a common factor (other than 1), we proceed by contradiction. Suppose p divides F_l and F_m, where $l < m$. Then p divides $F_0 F_1 \dots F_l \dots F_{m-1}$ and therefore p divides $F_m - 2$, by $(*)$, as well as F_m. But this is impossible: all Fermat numbers are odd so no number other than 1 divides both $F_m - 2$ and F_m. Hence no two Fermat numbers have a common factor greater than 1.

For the last part, note that every number can be written uniquely as a product of prime factors and that because the Fermat numbers are co-prime, each prime can appear in at most one Fermat number. Thus, since there are infinitely many Fermat numbers, there must be infinitely many primes.

Post-mortem

This question is largely about proof. The above solution has a proof by induction and a proof by contradiction. The last part could have been written as a proof by contradiction too.

The difficulty is in presenting the proof. It is not enough to understand your own proof: you have to be able to set it out so that it is clear to the reader. This is a vital part of mathematics and its most useful transferable skill.

At the meeting in which this question was first considered, one of the examiners said that he didn't see the point of the question, since there is already a well-known proof (due to Euclid, possibly) that there are infinitely many primes. As mentioned overleaf, this proof is due to Goldbach, and I could only respond that if Goldbach thought it worthwhile, that was good enough for me.