

Factoring Fermat Numbers

A Unique Computational Experiment for Factoring F_9

C E Veni Madhavan

Fermat observed that the numbers $F_k = 2^{2^k} + 1$, $k = 0, 1, 2, 3, 4$ are prime, and wondered whether this was true for all k . Euler found that the very next Fermat number is composite: $F_5 = 2^{32} + 1 = 641 \times 6700417$. So far it has been verified that F_k , $5 \leq k \leq 22$ are all *composite*. No one knows whether any other F_k is prime. The numbers F_k grow rapidly with k — each is almost a square of the previous number — and it is a very difficult task to decide their primality. We give below an outline of the relevant computational challenges.

First note that, if k is odd, 3 divides $2^k + 1$ and in general, $2^a + 1$ divides $2^{ak} + 1$. Thus, if k is not a power of two, $2^k + 1$ is not prime. Fermat hazarded a guess that the converse was also true. In 1877, François Pépin published a necessary and sufficient condition which states that F_k , $k > 1$ is prime if and only if F_k divides $5^{(F_k - 1)/2} + 1$. This condition is the basis for determining whether F_k is prime for any given k . Failure of this condition means that F_k is composite. It does not reveal any information about the factors.

Today, sophisticated number theoretic methods and powerful computing platforms are used for testing primality and factoring of large integers. These find applications in many practical

problems such as cryptography. The recent records in Fermat number factoring have been achieved by means of two techniques called *number field sieve* (NFS) and *elliptic curve method* (ECM).

The complete factoring of F_9 , which has about 150 decimal digits was carried out in 1992 by a unique computational experiment. Hundreds of computers in different parts of the world, working independently and in their spare time generated certain seed numbers. These computers sent their seeds by electronic mail to a host computer in USA. The host carried out the combination of the seeds and the factoring. The NFS method, requiring the generation of an enormous number of such seeds, was thus eminently suitable for this exercise. However this method is quite difficult to implement.

Last year the number F_{22} was determined to be composite, using Pépin's criterion and extremely fast arithmetical algorithms implemented on supercomputers. This number of about 1.3 million decimal digits (about 500 times as long as this article) required about 10^{16} arithmetical operations and about seven months of real time. Complete factorization of Fermat numbers is known only for $k \leq 9$ and $k = 11$. No prime factors of F_{14} and F_{20} are known.

C E Veni Madhavan is with the Department of Computer Science and Automation, Indian Institute of Science, Bangalore 560 012.

