Fermat numbers

Canonical name	FermatNumbers
Date of creation	2013-03-22 11:42:46
Last modified on	2013-03-22 11:42:46
Owner	drini (3)
Last modified by	drini (3)
Numerical id	30
Author	drini (3)
Entry type	Definition
Classification	msc 81T45
Classification	msc 81T13
Classification	msc 11A51
Classification	msc 20L05
Classification	msc 46L87
Classification	msc 43A35
Classification	msc 43A25
Classification	msc 22D25
Classification	msc 55U40
Classification	msc 18B40
Classification	msc 46L05
Classification	msc 22A22
Classification	msc 81R50
Classification	msc 55U35
Defines	Fermat prime

The n-th *Fermat number* is defined as:

$$F_n = 2^{2^n} + 1.$$

Fermat incorrectly conjectured that all these numbers were primes, although he had no proof. The first 5 Fermat numbers: $3, 5, 17, 257, 65537$ (corresponding to $n = 0, 1, 2, 3, 4$) are all primes (so called Fermat primes) Euler was the first to point out the falsity of Fermat's conjecture by proving that 641 is a divisor of F_5. (In fact, $F_5 = 641 \times 6700417$). Moreover, no other Fermat number is known to be prime for $n > 4$, so now it is conjectured that those are all prime Fermat numbers. It is also unknown whether there are infinitely many composite Fermat numbers or not.

One of the famous achievements of Gauss was to prove that the regular polygon of m sides can be constructed with ruler and compass if and only if m can be written as

$$m = 2^k F_{r_1} F_{r_2} \cdots F_{r_t}$$

where $k \geq 0$ and the other factors are distinct primes of the form F_n (of course, t may be 0 here, i.e. $m = 2^k$ is allowed).

There are many interesting properties involving Fermat numbers. For instance:

$$F_m = F_0 F_1 \cdots F_{m-1} + 2$$

for any $m \geq 1$, which implies that $F_m - 2$ is divisible by all smaller Fermat numbers.

The previous formula holds because

$$F_m - 2 = (2^{2^m} + 1) - 2 = 2^{2^m} - 1 = (2^{2^{m-1}} - 1)(2^{2^{m-1}} + 1) = (2^{2^{m-1}} - 1)F_{m-1}$$

and expanding recursively the left factor in the last expression gives the desired result.

References.

Krízek, Luca, Somer. *17 Lectures on Fermat Numbers.* CMS Books in Mathematics.