Fermat number primality testing algorithm

Author engineer Sergio Adrián Martín

Introduction

The so-called Fermat numbers are an infinite set of numbers that respond to the following equation for every value of n integer

$$F(n)=2^{(2^n)}+1 \quad (1)$$

Pierre de Fermat created this formula arguing that all the numbers it originates would be prime. However, a generation later it was found that what should be Fermat's sixth prime number was not.
In a previous work I explained the form that all numbers that could possibly divide a Fermat number should have.
Using a probabilistic argument I stated that the chances of finding an integer that divided a Fermat number grew exponentially as the Fermat number became larger, hence the probability of finding a sixth Fermat prime would be zero.
However, this reasoning, although logical, is not absolutely conclusive, unless it is shown that for n greater than or equal to five, every Fermat number generated is a composite number.
The 100% sure method of checking that a Fermat number is composite involves dividing it by one of its possible divisors, but this task becomes particularly difficult unless you have a computer capable of handling more than 40 digits in each division.
This exceeds the capacity of practically all desktop computers, and limits the possibilities of delving deeper into this topic, unless you have computers with a high capacity for arithmetic operations.
However, the purpose of this work is to present a method that guarantees that the primality of a large fermat number can be tested, even without powerful computing equipment.

Base of Fermat dividers

the equation equation of Proth's theorem

$$C=\frac{2^{\frac{(p-1)}{2}}+1}{p} \quad (2)$$

C will be integer at least in 50% of the cases, when p is prime.
If you replace the exponent in the following way

$$q2^n=\frac{(p-1)}{2} \quad (3)$$

we arrive at the following equation

$$C=\frac{2^{q2^n}+1}{q2^{(n+1)}+1} \quad (4)$$

The numerator of this expression can be factorized,

$$2^{q2^n}+1=\left(2^{2^n}+1\right)\left(\sum_{k=0}^{q-1}(-1)^k 2^{k2^n}\right) \quad (5)$$

This means that there is a 50% chance that the following quotient is an integer.