Fermat Numbers

Preprint · January 2020

DOI: 10.13140/RG.2.2.31221.73449

Mercedes Orús-Lacort
Universitat Autònoma de Bsrcelona - UAB

Fermat numbers are not prime numbers for $n \geq 5$

Mercedes Orús–Lacort
Online teacher of College Mathematics

January 20, 2020

Abstract

In this paper we show a demonstration which allow us to prove how the Fermat numbers $2^{2^n}+1$ are not prime numbers for $n \geq 5$. In particular, using Édouard Lucas result, we show that for $n \geq 5$, $2^{2^n}+1$ can be written as $(k_1 \cdot 2^{n+2}+1) \cdot k_2$ for k_1 and k_2 positive integer numbers.

Key Words: Number theory, Fermat Numbers.

AMS Classification: 11–02

1 Introduction

In mathematics are well known Fermat numbers, being Pierre the Fermat the first who studied them.

These numbers can be written as:

$$F_n = 2^{2^n} + 1 \text{ for } n \in \mathbb{N}$$

Fermat numbers were first studied by Pierre de Fermat, who conjectured that all Fermat numbers are prime.

The first five Fermat numbers F_0,... F_4 are prime. However, the conjecture was refuted by Leonhard Euler in 1732 when he showed that:

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

Euler proved that every factor of F_n must have the form $k \cdot 2^{n+1}+1$, and later it was improved by Édouard Lucas to $k \cdot 2^{n+2}+1$, for $k \in \mathbb{N}$.

F_n for $n < 5$ are prime numbers, and it seems that there are no other known Fermat primes F_n with $n \geq 5$. However, little is known about Fermat numbers with large n [1].

In fact, each of the following was an open problem:

- Is F_n composite for all $n > 4$?.

- Are there infinitely many Fermat primes? (Eisenstein 1844) [2].
- Are there infinitely many composite Fermat numbers?.

As of 2014, it is known that F_n is composite for $5 \leq n \leq 32$, although only is known the complete factorizations of F_n for $0 \leq n \leq 11$, and there are no known prime factors for $n = 20$ and $n = 24$ [3]. The largest Fermat number known to be composite is $F_{3329780}$, and its prime factor $193 \cdot 23329782 + 1$, a megaprime, was discovered by the PrimeGrid collaboration in July 2014 [3] [4].

The distributed computing project Fermat Search is searching for new factors of Fermat numbers [5]. The set of all Fermat factors is A050922 (or, sorted, A023394) in OEIS.

It seemed then possible that the only primes of this form are 3, 5, 17, 257 and $65,537$. Indeed, Boklan and Conway published in 2016 a very precise analysis suggesting that the probability of the existence of another Fermat prime is less than one in a billion [6].

In this paper we show a demonstration which allow us to prove how the Fermat numbers $2^{2^n}+1$ are not prime numbers for $n \geq 5$. In particular, using Édouard Lucas result, we show that for $n \geq 5$, $2^{2^n}+1$ can be written as $(k_1 \cdot 2^{n+2}+1) \cdot k_2$ for k_1 and k_2 positive integer numbers.

The paper is organized as follows: in Sec.2 we show a demonstration which allow us to prove how the Fermat numbers $2^{2^n}+1$ are not prime numbers for $n \geq 5$. In Sec.3 we wrap up our conclusions.

2 Fermat numbers $2^{2^n}+1$ are not prime numbers for $n \geq 5$

It is well known that $F_n = 2^{2^n}+1$ is a prime number for $0 \leq n \leq 4$, but it seems that for $n \geq 5$ are not prime numbers.

Lucas showed that if F_n is not a prime number, then every factor must have the form $k \cdot 2^{n+2}+1$ for $k \in \mathbb{N}$ and $k > 0$.

Hence, we will show what condition must satisfy n, so that, F_n can be factored as $2^{2^n}+1 = (k_1 \cdot 2^{n+2}+1) \cdot k_2$, for k_1 and k_2 natural numbers greater than zero.

Let $f(x) = F_x = 2^{2^x}+1$ and $g(x) = (k_1 \cdot 2^{x+2}+1) \cdot k_2$ be two functions both from $\mathbb{R}$ to $\mathbb{R}$.

First, we will analyze what condition must satisfy x so that $f'(x) = g'(x)$.

$$
\begin{aligned}
&f'(x) = 2^{2^x} \cdot 2^x \cdot (\ln(2))^2 \\
&g'(x) = 4 \cdot k_1 \cdot k_2 \cdot 2^x \cdot \ln(2) \\
&2^{2^x} \cdot 2^x \cdot (\ln(2))^2 = 4 \cdot k_1 \cdot k_2 \cdot 2^x \cdot \ln(2) \\
&2^{2^x} \cdot \ln(2) = 4 \cdot k_1 \cdot k_2 \\
&2^{2^x} = \frac{4 \cdot k_1 \cdot k_2}{\ln 2} \\
&2^x \cdot \ln(2) = \ln(\frac{4 \cdot k_1 \cdot k_2}{\ln 2}) \\
&2^x = \frac{\ln(\frac{4 \cdot k_1 \cdot k_2}{\ln 2})}{\ln(2)} \\
&x \cdot \ln(2) = \ln(\frac{\ln(\frac{4 \cdot k_1 \cdot k_2}{\ln 2})}{\ln(2)}) \\
&x = \frac{\ln(\frac{\ln(\frac{4 \cdot k_1 \cdot k_2}{\ln 2})}{\ln(2)})}{\ln(2)}
\end{aligned} \tag{1}
$$

Since $F_5 = 4294967297$, then $k_1 > 1$, and if we consider $k_1 = 2$ and $n = 5$, then $(2 \cdot 2^7 + 1) = 257$, hence $k_2 > 10000$, for instance.

Hence, using these conditions for k_1 and k_2, we have:

$$
x = \frac{\ln(\frac{\ln(\frac{4 \cdot k_1 \cdot k_2}{\ln 2})}{\ln(2)})}{\ln(2)} \geq \frac{\ln(\frac{\ln(\frac{80000}{\ln 2})}{\ln(2)})}{\ln(2)} = 4.07... \tag{2}
$$

That is, if $x \geq 4.07...$ we have $f'(x) = g'(x)$, that is, $f(x) + C = g(x) + D$, and since $F_5 = 4294967297 = f(5) + C = 2^{2^5} + 1 + C$ and $4294967297 = 2^{2^5} + 1$, this implies $C = 0$, and on the other hand since $F_5 = 4294967297 = f(5) = g(5) + D =$ and $4294967297 = 641 \cdot 6700417 = (5 \cdot 2^7 + 1) \cdot 6700417 = g(2)$, this implies $D = 0$.

Hence $C = D = 0$, and then, if x is greater or equal to 4.07... we have $f(x) = g(x)$.

And if we consider now $f(x)$ and $g(x)$ over the natural numbers, we have: If n is greater or equal to 5 then $f(n) = g(n)$ for $n \in \mathbb{N}$.

Therefore, if n is greater or equal to 5, F_n is not prime, it can be factored as $2^{2^n} + 1 = (k_1 \cdot 2^{n+2} + 1) \cdot k_2$ for k_1 and k_2 natural numbers.

3 Conclusions

We have shown how to prove that Fermat numbers $2^{2^n} + 1$ are not prime numbers for $n \geq 5$. In particular, using Édouard Lucas result, we show that for $n \geq 5$, $2^{2^n} + 1$ can be written as $(k_1 \cdot 2^{n+2} + 1) \cdot k_2$ for k_1 and k_2 positive integer numbers.

Acknowledgements: we acknowledge Roman Orus and Christophe Jouis for proposing the dissemination of this result.

References

[1] Grytczuk, A.; Luca, F. and Wójtowicz, M. (2001), "Another note on the greatest prime factors of Fermat numbers", Southeast Asian Bulletin of Mathematics, 25 (1): 111–115, doi:10.1007/s10012-001-0111-4

[2] Guy, Richard K. (2004), Unsolved Problems in Number Theory, Problem Books in Mathematics, 1 (3rd ed.), New York: Springer Verlag, pp. A3, A12, B21, ISBN 978-0-387-20860-2

[3] Křížek, Michal; Luca, Florian and Somer, Lawrence (2001), 17 Lectures on Fermat Numbers: From Number Theory to Geometry, CMS books in mathematics, 10, New York: Springer, ISBN 978-0-387-95332-8 - This book contains an extensive list of references.

[4] Křížek, Michal; Luca, Florian and Somer, Lawrence (2002), "On the convergence of series of reciprocals of primes related to the Fermat numbers" (PDF), Journal of Number Theory, 97 (1): 95–112, doi:10.1006/jnth.2002.2782

[5] Luca, Florian (2000), "The anti-social Fermat number", American Mathematical Monthly, 107 (2): 171–173, doi:10.2307/2589441, JSTOR 2589441

[6] Ribenboim, Paulo (1996), The New Book of Prime Number Records (3rd ed.), New York: Springer, ISBN 978-0-387-94457-9

Email: mercedes.orus@gmail.com