Fermat Numbers, Goldbach's Theorem, and the Infinitude of the Primes

Reilly Leblanc, AJ Liberatore, Eli Sanderson

Dr. John Haga

Wentworth Institute of Technology

Primality of Fermat Numbers

Fermat numbers are a set of positive integers of the form $2^{2^n}+1$ studied extensively by several notable mathematicians throughout history, including Pierre de Fermat, Leonhard Euler, Christian Goldbach, and many others. In 1640, Fermat proposed his claim about what we now call Fermat numbers in letters addressed to mathematicians and other great thinkers at the time, proposing that such numbers must be prime. However, around a century later, Euler proved that 641 is a factor of $2^{2^5}+1$, leading to further investigation. In the modern day, mathematicians are still unsure if any Fermat numbers for n greater than 4 are prime, given only Fermat numbers up to n = 30 have been investigated, and none of them are prime.

Works Cited

1. Larson, Ron; Hostetler, Robert P.; Edwards, Bruce H. (2008). *Essential Calculus: Early Transcendental Functions*. Boston: Houghton Mifflin.
2. Dunham, William (1999). *Euler: The Master of Us All*. Mathematical Association of America.
3. Křížek, Michal; Luca, Florian & 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
4. Golomb, S. W. (January 1, 1963), "On the sum of the reciprocals of the Fermat numbers and related irrationalities", *Canadian Journal of Mathematics*, **15**: 475–478

Definitions

Definition 1. $\mathbb{N}$ is the set of Natural numbers $\{0, 1, 2, 3, \dots\}$

Definition 2. A Fermat number, denoted F_n, is a positive integer of the form $F_n = 2^{2^n}+1, n \in \mathbb{N}$. Thus, the first few Fermat numbers are as follows:

$$3,\ 5,\ 17,\ 257,\ 65537\dots$$

Properties

Property 1. Any Fermat number can be written as the product of the previous Fermat numbers plus two: $F_n = F_0F_1\dots F_{n-1}+2$ for $n \geq 1, n \in \mathbb{N}$.

Proof. We proceed by mathematical induction, when $n = 1$, the statement becomes: $F_1 \stackrel{?}{=} F_0 + 2$. By computation, the LHS is $F_1 = 2^{2^1}+1 = 2^2+1 = 5$ and the RHS is $(2^{2^0}+1)+2 = (2+1)+2 = 5$. Thus when $n = 1$ the statement is true.

Assuming the inductive hypothesis, $F_n = F_0F_1\dots F_{n-1}+2$ for some $n \geq 1$. From this we can deduce that $F_0F_1\dots F_{n-1} = F_n - 2$. Now consider the expression $F_0F_1\dots F_{n-1}F_n + 2$. We may write this as $(F_n-2)F_n+2 = (2^{2^n}-1)(2^{2^n}+1)+2$. By algebra the expression becomes $2^{2^{n+1}}+1$ which is the exact form of the F_{n+1} Fermat number. Thus the statement is true for $n+1$, so by mathematical induction the statement is true $\forall n \in \mathbb{N} \mid n \geq 1$ □

Property 2. Any Fermat number can be rewritten as the sum of the previous term and the product of $2^{2^{n-1}}$ and all previous terms of an index at least 2 less than said Fermat number: $F_n = F_{n-1} + 2^{2^{n-1}}F_0\cdots F_{n-2}$ for $n \geq 2, n \in \mathbb{N}$

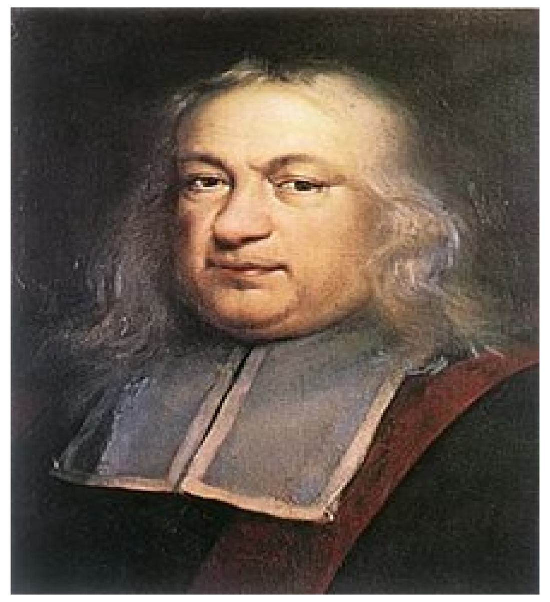
Proof. We proceed by mathematical induction. When $n = 2$, the statement becomes $F_1 + 2^{2^1}F_0 = 5 + 4 * 3 = 17 = F_2$. Thus the base case is proven.

Inductive Hypothesis: Suppose the statement is true for some natural number $n \in \mathbb{N}$ with $n \geq 2$. Thus, we have $F_n = F_{n-1} + 2^{2^{n-1}}F_0\cdots F_{n-2}$ for $n \geq 2, n \in \mathbb{N}$.

Now, consider $F_{n+1} - F_n$. By definition of Fermat Numbers, we may rewrite this expression as follows:

$$\begin{aligned} F_{n+1} - F_n &= (2^{2^{n+1}}+1) - (2^{2^n}+1) \\ &= 2^{2^{n+1}} - 2^{2^n} \\ &= 2^{2^n}\left(2^{2^n}-1\right) \\ &= 2^{2^n}\left((2^{2^n}+1)-2\right) \\ &= 2^{2^n}\left(F_n-2\right) \\ F_{n+1} - F_n &= 2^{2^n}F_0\cdots F_{n-1} \end{aligned}$$

Thus, we have that our original statement, $F_{n+1} - F_n$, is equivalent to $2^{2^n}F_0\cdots F_{n-1}$, which is precisely what we were seeking. Therefore, by P.M.I, the statement is true for all $n \in \mathbb{N}$ with $n \geq 2$. □



Pierre de Fermat
1607-1665
French Mathematician who is given credit for early developments that led to infinitesimal calculus

Leonhard Euler
1707-1783
Swiss Mathematician, known for helping develop infinitesimal calculus and graph theory.

Goldbach's Theorem

Claim. No two Fermat numbers share a common integer factor greater than 1.

Proof. Assume to the contrary that there exists a prime number $a \in \mathbb{Z}$ *s.t.* $a \mid F_i$ and $a \mid F_j$, where $a > 1$ and F_i, F_j are two distinct Fermat numbers. Also, without loss of generality, assume that $F_i > F_j$. By property 2 $F_i = F_{i-1} + 2^{2^{i-1}}F_0\dots F_j\dots F_{i-2}$ Since a divides F_i and F_j, a also divides F_{i-1}. Hence we may state that a divides $F_0\dots F_j\dots F_{i-1}$. It follows that a divides the difference $F_i - F_0\dots F_j\dots F_{i-1}$, which from property 1 is equal to 2, thus $p = 2$. However, all Fermat numbers are odd, as they take the form of an even number, $2^n \mid n \in \mathbb{N}$, plus one. This is a contradiction, thus no two Fermat numbers share a common integer factor greater than 1. □

Corollary. There are infinitely many primes.

Proof. The definition of a Fermat number states that there exists a Fermat number for every natural number n greater than or equal to 2. There are infinitely many natural numbers n greater than or equal to 2; thus, it is the case that there are infinitely many Fermat numbers. Given Goldbach's theorem, no two Fermat numbers share a common integer factor greater than 1. Since all Fermat numbers are relatively prime, such that they share no common integer factors greater than 1, and there are infinitely many Fermat numbers, it must be the case that there are infinitely many primes so that all Fermat numbers have a prime factorization (which must be true, given the Fundamental Theorem of Arithmetic). □

'n'	Fermat Number = 2^(2^n) + 1	Prime?
0	3	Yes
1	5	Yes
2	17	Yes
3	257	Yes
4	65,537	Yes
5	4,294,967,297	No
6	18,446,744,073,709,600,000	No
...	...as far as has been calculated...	...No...

A table of Fermat numbers