Note on the Fascinating Fermat Numbers

Mulatu Lemma, Noel Mengistie and Samera Mulatu
Department of Mathematics
Savannah, GA 31404
USA

Abstract: A Fermat number is an integer of the form

$$F_n = 2^{2^n} + 1 \qquad n \geq 0$$

The Fermat numbers are named after the French mathematician Pierre de Fermat (1601 – 1665) who first studied numbers of such form.
In this paper we investigated some interesting properties of the Fermat numbers.
The first five Fermat numbers are 1,5,17,257 and 65537.

The Main Results

The following two theorems deal with the recursive properties of the Fermat Numbers.

Theorem 1. $F_{n+1} = (F_n - 1)^2 + 1$ for $n \geq 0$

Proof:

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

Example 1: Note that

$$F_3 = (F_2 - 1)^2 + 1$$

$$= \left(2^{2^2} - 1 + 1\right)^2 + 1$$
$$= \left(2^{2^2}\right)^2 + 1$$
$$= 2^{2^3} + 1$$
$$= 2^8 + 1$$
$$= 257$$

Theorem 2. $F_n = F_0 \ldots F_{n-2} \cdot F_{n-1} + 2$ for $n \geq 1$

<u>Proof:</u> We use induction n

Step 1: $n = 1$ holds as

$$F_0 + 2 = 3 + 2 = 5 = F_1$$

Step 2: Assume the hypothesis is true $n = k$ that is

$$F_0 \ldots F_{k-1} + 2 = F_k$$

Step 3: Prove that the hypothesis holds for $n = k + 1$. We have

$$\begin{aligned} F_0 \ldots F_k + 2 &= F_0 \ldots F_{k-1} \cdot F_k + 2 \\ &= (F_k - 2) \cdot F_k + 2 \\ &= \left(2^{2^k} + 1 - 2\right)\left(2^{2^k} + 1\right) + 2 \\ &= \left(2^{2^k} - 1\right)\left(2^{2^k} + 1\right) + 2 \\ &= 2^{2^{k+1}} - 1 + 2 \\ &= 2^{2^{k+1}} + 1 \\ &= F_{k+1} \end{aligned}$$

<u>Example 2:</u> Observe that

$$\begin{aligned} F_3 &= F_0 \cdot F_1 + F_2 + 2 \\ &= 3 \cdot 5 + 17 + 2 \\ &= 255 + 2 \\ &= 257 \end{aligned}$$

Corollary 1: For $n \geq 1$, we have

$$F_n = 2(\bmod F_m) \quad \text{for all} \quad m = 0,1,\ldots,n-1$$

Proof: Easily follows by Theorem 2

Corollary 2: For $n \geq 2$, we have the last digit of $F_n = 7$

Proof: From Corollary 1, we have

$$F_n = 2(\bmod 5)$$

$$\Rightarrow F_n = 2(\bmod 5) \quad \text{as all } F_n \text{ are odd}$$

$$\Rightarrow \text{the last digit of } F_n = 7$$

Theorem 3. Every F_n is of the form

$$6k - 1 \text{ for } n \geq 1$$

Proof: Note by Theorem 2,

$$F_{n+1} = F_0 \cdot F_1 \ldots F_n + 2 + 1$$

$$= 3 \cdot F_1 \ldots F_n + 3$$

$$= 3(F_1 \ldots F_n + 1)$$

$F_1 \ldots F_n$ is odd $\Rightarrow F_1 \ldots F_n + 1$ is even and hence

$$F_{n+1} = 3 \cdot 2k = 6k$$

$$\Rightarrow F_n = 6k - 1$$

Remark 1. The first five Fermat numbers 1,5,17,257 and 65537 are all primes. A question must be raised if all Fermat numbers are primes. But this is not true as shown by the following theorem. We give our own new proof to this theorem.

Theorem 4. The Fermat number $F_5 =$ 4,294,967,297 is divisible by 641

Proof: Observe that $641 = 5 \cdot 2^7 + 1$ and $F_5 = 2^{3^2} + 1$. Now we have

$$5 \cdot 2^7 \equiv -1(\bmod 641)$$

$$\Rightarrow \left(5\cdot 2^{7}\right)^{4} \equiv -1^{4} \pmod{641}$$
$$\Rightarrow 5^{4}\cdot 2^{28} \equiv 1 \pmod{641}$$
$$\Rightarrow 625\cdot 2^{28} \equiv 1 \pmod{641}$$
$$\Rightarrow (-16)\cdot 2^{28} \equiv 1 \pmod{641}$$
$$\Rightarrow 16\cdot 2^{28} \equiv -1 \pmod{641}$$
$$\Rightarrow 2^{4}\cdot 2^{28} \equiv -1 \pmod{641}$$
$$\Rightarrow 2^{32} \equiv -1 \pmod{641}$$
$$\Rightarrow 2^{32}+1 \equiv 0 \pmod{641}$$
$$\Rightarrow 641 \mid \left(2^{32}+1\right)$$
$$\Rightarrow 641 \mid F_5$$

Theorem 5. The Fermat numbers are relatively prime to each other.

Proof: Let F_m and F_n be two Fermat numbers, where $m > n \geq 0$. Let $d = \gcd(F_n, F_m)$. Observe that Fermat numbers are odd numbers, $\gcd(F_n, F_m)$ must be odd. That is d is odd.

Let $x = 2^{2^n}$ $k = 2^{m-n}$, then

$$\frac{F_m - 2}{F_n} = \frac{\left(2^{2^n}\right)^{m-n} 2 - 1}{2^{2^n}+1}$$
$$= \frac{x^k - 1}{x+1} = x^{k-1} - x^{k-2} + \ldots + 1$$
$$\Rightarrow F_n\left(F_m - 2\right) \Rightarrow d \mid P_n \Rightarrow d \mid \left(F_m - 2\right)$$
$$\Rightarrow d \mid 2 \text{ as } d \mid m \Rightarrow d = 1$$

We state the following Pepin’s Test as Theorem 3 without proof and use it.

Theorem 6. Pepin’s Test. For $n \geq 1$, the Fermat number $F_n = 2^{2^n}+1$ is prime $\Leftrightarrow 3^{(F_{n-1})/2} \equiv -1 \bmod (F_n)$

Corollary 3. Using Pepin’s Test prove that $F_3 = 257$ is prime. Note that

Proof

$$3^{(F_{3-1})/2} \equiv 3^{128} = 3^3(5)^{25}$$
$$\equiv 27(-14)^{25}$$
$$\equiv 27\cdot 14^{24}(-14)$$
$$\equiv 27(17)(-14)$$
$$\equiv 27\cdot 19 \equiv 513 \equiv -1 \pmod{257}$$
$$\Rightarrow F_3 \quad \text{Is prime.}$$

Theorem 7. No Fermat number F_n for $n \geq 2$ can be expressed as the sum of two primes.

***Proof*.** We use proof By Contradiction**.** Assume that there exists $n \geq 2$ such that F_n could be expressed as the sum of two primes. Observe that since F_n is odd, one of the primes must be 2. Then the other prime would equal $F_n - 2 = F_n - 2 = 2^{2^n} - 1 = (2^{2^{n-1}} + 1)(2^{2^{n-1}} - 1)$ which is not a prime

Acknowledgments. Special Thanks to:
1. Aster Debebe
2. Zenaye Mengistie
3. Tadesse Dejene
4. Yohannis Debebe
5. Genet Wondimu
6. Asrat Worku
7. Beruke Debebe

References:

1. Burton, D. M. (1998). *Elementary number theory*. New York City, New York: McGraw-Hill.
2. Dodge, C. W. (1975). *Numbers and mathematics*. Boston, Massachusetts: Prindle, Weber & Schmidt Inc..
3. Dudley, Underwood (1969). *Elementary number theory*. San Francisco: W. H. Freeman and Company.
4. Jackson, T. H. (1975). *Number theory*. Boston, Massachusetts: Rouledge & Kegan Paul Ltd..