Fermat Numbers

Cindy Tsang
University of Washington

Math414 Number Theory
Professor William Stein
March 12, 2010

0 Content

1 Introduction

Prime numbers are widely studied in the field of number theory. One approach to investigate prime numbers is to study numbers of a certain form. For example, it has been proven that there are infinitely many primes in the form $a + nd$, where $d \geq 2$ and $\gcd(d, a) = 1$ (Dirichlet's theorem). On the other hand, it is still an open question to whether there are infinitely many primes of the form $n^2 + 1$.

In this paper, we will discuss in particular numbers of the form $2^{2^n} + 1$ where n is a nonnegative integer. They are called Fermat numbers, named after the French mathematician Pierre de Fermat (1601 – 1665) who first studied numbers in this form. It is still an open problem to whether there are infinitely many primes in the form of $2^{2^n} + 1$. We will not be able to answer this question in this paper, but we will prove some basic properties of Fermat numbers and discuss their primality and divisibility. We will also briefly mention numbers of the form $2^n - 1$ where n is a positive integer. They are called Mersenne numbers, named after the French mathematician Marin Mersenne. In section6, we will see how Mersenne numbers relate to the primality of Fermat numbers.

Pierre de Fermat (1601 – 1665)

Marin Mersenne (1588 – 1648)

[pictures from http://en.wikipedia.org/Pierre_de_Fermat & http://en.wikipedia.org/wiki/Marin_Mersenne]

2 Background of Fermat Numbers[1]

Fermat first conjectured that all the numbers in the form of $2^{2^n}+1$ are primes. However, in 1732, Leonhard Euler refuted this claim by showing that $F_5 = 2^{32} + 1 = 4{,}294{,}967{,}297 = 641 \times 6{,}700{,}417$ is a composite. It then became a question to whether there are infinitely many primes in the form of $2^{2^n}+1$. Primes in this form are called Fermat primes. Up-to-date there are only five known Fermat primes. (See section4 for more details on the current status of Fermat numbers.)

Leonhard Paul Euler (1707 – 1783)

Carl Friedrich Gauss (1977 – 1855)

[pictures from http://en.wikipedia.org/wiki/Euler & http://en.wikipedia.org/wiki/Gauss]

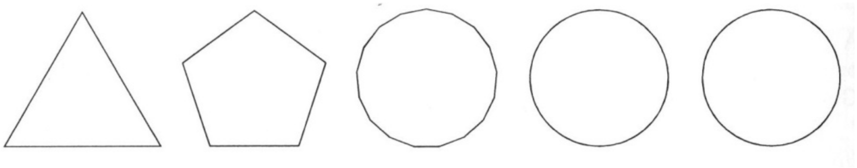
In 1796, the German mathematician Carl Friedrich Gauss (1977 – 1855) found an interesting relationship between the Euclidean construction (i.e. by ruler and compass) of regular polygons and Fermat primes. His theorem is known as Gauss's Theorem.

***Gauss's Theorem*[2].** There exists an Euclidean construction of the regular n-gon if and only if $n = 2^i p_1 p_2 \cdots p_j$, where $n \geq 3$, $i \geq 0$, $j \geq 0$, and $p_1, p_2, \ldots, p_j$ are distinct Fermat primes.

[1] All historical information in this section is from Reference1 Chapter1.

[2] A proof of Gauss's Theorem can be found in Reference1 Chapter16.

Gauss’s theorem implies that all 2^n-gons for $n \geq 2$ are constructible. Moreover, since so far only five Fermat numbers are known to be prime, it implies that for n odd, there are only ${}_5C_1 + {}_5C_1 + {}_5C_1 + {}_5C_1 + {}_5C_1 = 31$ n-gons that are known to be Euclidean constructible. If it turns out that there is only a finite number of Fermat primes, then this theorem would imply that there is only a finite number of Euclidean constructible n-gons for n odd. The figure below shows five Euclidean constructible n-gons.



Triangle, pentagon, heptadecagon, 257-gon and 65537-gon.
[figure from Reference1 Chapter4]

3 Geometric Interpretation of Fermat Numbers

As Gauss's theorem suggests, Fermat numbers might be closely related to some of the problems in Geometry. It is hence useful if we can understand what they mean geometrically.

A Fermat number $F_n = 2^{2^n} + 1$ (for $n \geq 1$) can be thought of as a square whose side length is $2^{2^{n-1}}$ plus a unit square (see figure1). Hence, determining whether a (Fermat) number is a composite or not is equivalent to determining whether we can rearrange the unit-square blocks to form a rectangle (see figure2). Moreover, determining whether an integer *d* divides a (Fermat) number is the same as deciding whether we can reorganize the blocks to form a rectangle with base *d*; or alternatively, we can also think of it as determining whether we can "fill" the area with a number of $r \cdot d$ unit-square blocks for some integer *r* (see figure3).

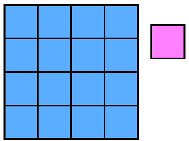


Figure1. $F_2 = 4^2 + 1 = 17$

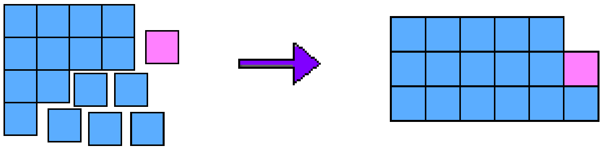


Figure2. $F_2 = 17$ is not a composite because no matter how you rearrange the blocks, you cannot get a rectangle.

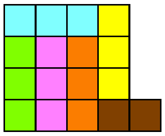


Figure3. $F_2 = 17$ is not divisible by 3.

Some of the properties we will prove in section5 can be easily understood if we interpret them geometrically. The reader should pay close attention. We will also make remarks on several of them.

4 Factoring Status of Fermat Numbers[3] (as of February 3, 2010)

The below table only shows the factoring status of Fermat numbers up to $n = 200$. For larger Fermat numbers and other details, see http://www.prothsearch.net/fermat.html#Summary.

Prime	🟨
Composite with no known factors	🟩
Composite with complete factorization	🟦
Composite with incomplete factorization	🟪
Unknown	🟥

									🟨 0
🟨 1	🟨 2	🟨 3	🟨 4	🟦 5	🟦 6	🟦 7	🟦 8	🟦 9	🟦 10
🟦 11	🟪 12	🟪 13	🟪 14	🟪 15	🟪 16	🟪 17	🟪 18	🟪 19	🟩 20
🟦 21	🟩 22	🟪 23	🟩 24	🟪 25	🟪 26	🟪 27	🟪 28	🟪 29	🟪 30
🟪 31	🟪 32	🟥 33	🟥 34	🟥 35	🟪 36	🟪 37	🟪 38	🟪 39	🟥 40
🟥 41	🟪 42	🟪 43	🟥 44	🟥 45	🟥 46	🟥 47	🟪 48	🟥 49	🟥 50
🟥 51	🟪 52	🟥 53	🟥 54	🟪 55	🟥 56	🟥 57	🟪 58	🟥 59	🟥 60
🟪 61	🟪 62	🟪 63	🟪 64	🟥 65	🟪 66	🟥 67	🟥 68	🟥 69	🟥 70
🟪 71	🟪 72	🟪 73	🟥 74	🟪 75	🟥 76	🟪 77	🟥 78	🟥 79	🟥 80
🟪 81	🟥 82	🟪 83	🟥 84	🟥 85	🟥 86	🟥 87	🟪 88	🟥 89	🟪 90
🟪 91	🟥 92	🟪 93	🟪 94	🟥 95	🟪 96	🟥 97	🟥 98	🟪 99	🟥 100
🟥 101	🟥 102	🟥 103	🟥 104	🟥 105	🟥 106	🟪 107	🟥 108	🟥 109	🟥 110
🟥 111	🟥 112	🟥 113	🟥 114	🟥 115	🟪 116	🟪 117	🟥 118	🟥 119	🟥 120
🟥 121	🟪 122	🟥 123	🟥 124	🟪 125	🟥 126	🟥 127	🟥 128	🟥 129	🟥 130
🟥 131	🟥 132	🟪 133	🟥 134	🟥 135	🟥 136	🟥 137	🟥 138	🟥 139	🟥 140
🟥 141	🟪 142	🟥 143	🟪 144	🟥 145	🟪 146	🟪 147	🟥 148	🟥 149	🟪 150
🟥 151	🟥 152	🟥 153	🟥 154	🟥 155	🟥 156	🟥 157	🟥 158	🟥 159	🟥 160
🟥 161	🟥 162	🟥 163	🟪 164	🟥 165	🟥 166	🟥 167	🟥 168	🟥 169	🟥 170
🟥 171	🟪 172	🟥 173	🟥 174	🟥 175	🟥 176	🟥 177	🟪 178	🟥 179	🟥 180
🟥 181	🟥 182	🟥 183	🟪 184	🟥 185	🟥 186	🟥 187	🟥 188	🟥 189	🟥 190
🟥 191	🟥 192	🟥 193	🟥 194	🟥 195	🟥 196	🟥 197	🟥 198	🟥 199	🟥 200

Total number of F_n primes known	5
Largest F_n prime known	$F_4 = 65537$
Total number of F_n composites known	243
Largest ten F_n composites known	F_{476624}, F_{495728}, F_{567233}, F_{585042}, F_{617813}, F_{67205}, F_{960897}, $F_{2145351}$, $F_{2167797}$, $F_{2478792}$

[3] All information from this section is from Reference2 http://www.prothsearch.net/fermat.html#Summary

5 Basic Properties of Fermat Numbers

In this section, we will prove some basic properties of Fermat numbers.

Theorem1[4]**.** For $n \geq 1$, $F_n = (F_{n\text{-}1} - 1)^2 + 1$.

Proof. $(F_{n\text{-}1} - 1)^2 + 1 = (2^{2^{n-1}} + 1 - 1)^2 + 1 = 2^{2^n} + 1 = F_n$ □

Remark1. This theorem is obvious if we interpret it geometrically:

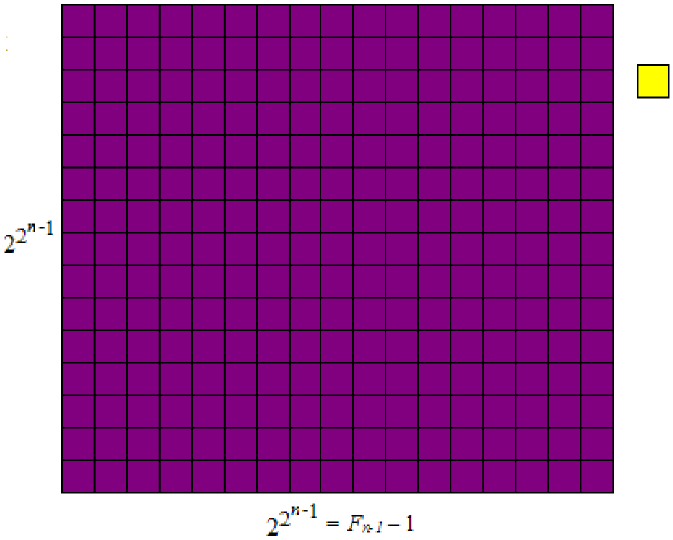


Figure4. Any Fermat number F_n is exactly a square with side length $F_{n\text{-}1} - 1$ plus a unit square.

Theorem2[5]**.** For $n \geq 1$, $F_n = F_0 \cdots F_{n\text{-}1} + 2$.

Proof. We will prove this by induction.

When $n = 1$, we have $F_0 + 2 = 3 + 2 = 5 = F_1$.

Now assume $F_n = F_0 \cdots F_{n\text{-}1} + 2$.

$$\begin{aligned} \text{Then, } F_0 \cdots F_n + 2 &= F_0 \cdots F_{n\text{-}1} \cdot F_n + 2 \\ &= (F_n - 2) \cdot F_n + 2 \qquad \text{(induction hypothesis)} \\ &= (2^{2^n} - 1) \cdot (2^{2^n} + 1) + 2 \\ &= 2^{2^{n+1}} + 1 = F_{n+1} \end{aligned}$$ □

[4] Theorem is found in Reference3. Proof is due to the author.

[5] Theorem is found in Reference3. Proof is due to the author.

Remark2. To understand the proof of Theorem2 geometrically, we can think of $F_n - 2$ as a square with side length $F_{n-1} - 1$ minus a unit square (see figure5). It is divisible by $F_{n-1} = 2^{2^{n-1}} + 1$ because we can form a rectangle by moving the top row and make it a column on the right (see figure6). To see that it is also divisible by F_{n-k} for $2 \le k \le n$, we can use the induction hypothesis that F_{n-k} divides $F_{n-1} - 2 = 2^{2^{n-1}} - 1$. It means that we can fill each column of the rectangle in figure5 evenly by $r{\cdot}F_{n-k}$ number of blocks for some integer r (see figure7).

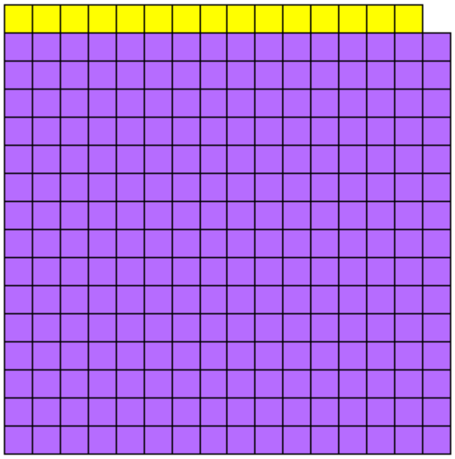


Figure5. A $2^{2^{n-1}}$ x $2^{2^{n-1}}$ square minus a unit square

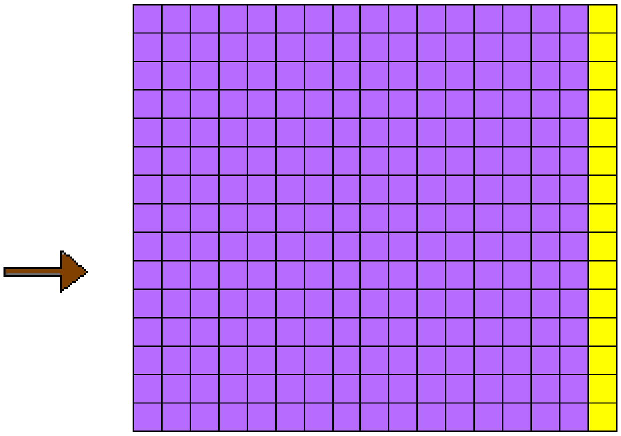


Figure6. A ($2^{2^{n-1}}$ – 1) x ($2^{2^{n-1}}$ + 1) rectangle

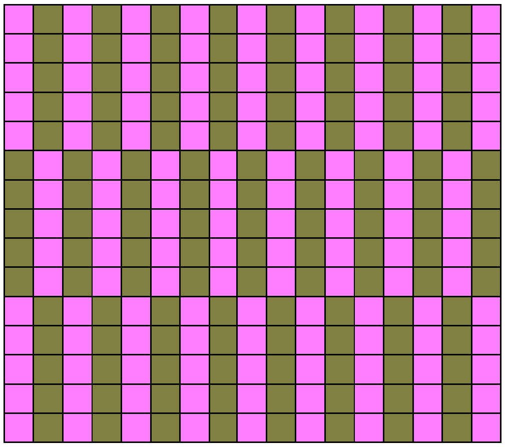


Figure7. Each column can be filled evenly by F_{n-k}.

Corollary2.1. [Reference1, p.27] For $n \ge 1$, $F_n \equiv 2$ (mod F_k) for all $k = 0, 1, \dots , n - 1$.

Proof. It is equivalent to say that $F_k \mid F_n - 2$, which is implied by Theorem2. □

Corollary2.2. [Reference1, p.28] For $n \ge 2$, the last digit of F_n is 7.

Proof. It follows directly from Corollary2.1 that $F_n \equiv 2$ (mod 5). Since all Fermat numbers are odd, it follows that $F_n \equiv 7$ (mod 10). □

Corollary2.3. No Fermat number is a perfect square.

Proof. $F_0 = 3$ and $F_1 = 5$ are obviously not a perfect square. For F_n where $n \geq 2$, by Corollary2.2, $F_n \equiv 7$ (mod 10). But only numbers that are congruent to *0, 1, 4, 5, 6,* or *9* (mod 10) can be a perfect square. □

Remark2.3. This is quite intuitive if we think of F_{n} as a square plus a unit square block. You can't possibly rearrange the block to form a perfect square.

Corollary2.4. [Reference1, p.31] Every Fermat number F_n for $n \geq 1$ is of the form $6m - 1$.

Proof. It is equivalent to show that $F_n + 1$ is divisible by 6. From Theorem2, we have $F_n + 1 = 3\cdot F_1\cdots F_n + 2 + 1 = 3\cdot(F_1\cdots F_n + 1)$, where $F_1\cdots F_n + 1$ is an even number. □

Theorem3[6]***.*** For $n \geq 2$, $F_n = F^2_{n-1} - 2\cdot(F_{n-2} - 1)^2$.

Proof. $F^2_{n-1} - 2\cdot(F_{n-2} - 1)^2 = (2^{2^{n-1}} + 1)^2 - 2\cdot(2^{2^{n-2}} - 1 + 1)^2$

$$= 2^{2^n} + 2\cdot 2^{2^{n-1}} + 1 - 2\cdot 2^{2^{n-1}}$$

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

□

[6] Theorem is found in Reference3. Proof is due to the author.

Theorem4[7]**.** For $n \geq 2$, $F_n = F_{n\text{-}1} + 2^{2^{n-1}} \cdot F_0 \cdots F_{n\text{-}2}$.

Proof. We will prove this by induction.

When $n = 2$, we have $F_1 + 2^2 \cdot F_0 = 5 + 2^2 \cdot 3 = 17 = F_2$.

Now assume $F_n = F_{n\text{-}1} + 2^{2^{n-1}} \cdot F_0 \cdots F_{n\text{-}2}$.

Then, $F_n + 2^{2^n} \cdot F_0 \cdots F_{n\text{-}1} = F_n + 2^{2^{n-1}} \cdot (2^{2^{n-1}} \cdot F_0 \cdots F_{n\text{-}2}) \cdot F_{n\text{-}1}$

$$= F_n + 2^{2^{n-1}} \cdot F_{n\text{-}1} \cdot (F_n - F_{n\text{-}1}) \qquad \text{(induction hypothesis)}$$

$$= 2^{2^n} + 1 + 2^{2^{n-1}} \cdot (2^{2^{n-1}} + 1) \cdot (2^{2^n} - 2^{2^{n-1}})$$

$$= 2^{2^n} + 1 + 2^{2^{n-1}} \cdot (2^{2^{n-1}} + 1) \cdot 2^{2^{n-1}} \cdot (2^{2^{n-1}} - 1)$$

$$= 2^{2^n} + 1 + 2^{2^n} \cdot (2^{2^n} - 1)$$

$$= 2^{2^n} + 1 + 2^{2^{n+1}} - 2^{2^n}$$

$$= 2^{2^{n+1}} + 1 = F_{n+1}$$

□

Theorem5. [Reference1, p.28] For $n \geq 2$, every Fermat number has infinitely many representations in the form $x^2 - 2y^2$, where x and y are both positive integers.

Proof. First, from Theorem3, $(x_0, y_0) = (F_{n-1}, F_{n-2} - 1)$ gives one such representation. Now notice that $(3x + 4y)^2 - 2 \cdot (2x + 3y)^2 = 9x^2 + 24xy + 16y^2 - 8x^2 - 24xy - 18y^2 = x^2 - 2y^2$. If x and y are both positive, then $3x + 4y > x$ and $2x + 3y > y$ are also positive. This means that we can find (x_i, y_i) recursively by setting $(x_i, y_i) = (3x_{i-1} + 4y_{i-1}, 2x_{i-1} + 3_{y-1})$. The set of all points (x_m, y_m) we find will be infinite, and each point will give a representation for F_n in the desired form. □

Theorem6. [Reference3] No two Fermat numbers share a common factor greater that 1.

Proof. Assume for contradiction that there exist F_i and F_j such that $a > 1$ divides both of them. Also, without loss of generality, assume that $F_j > F_i$.

From Theorem4, we know that $F_j = F_{j-1} + 2^{2^{j-1}} \cdot F_0 \cdots F_i \cdots F_{j-2}$. Since a divides F_i and F_j, a also divides F_{j-1} and hence $F_0 \cdots F_i \cdots F_{j-1}$. Then, a has to divide the difference $F_j - F_0 \cdots F_{j-1}$, which equals 2 by Theorem2. It follows that $a = 2$, but all Fermat numbers are obviously odd. □

[7] Theorem is found in Reference3. Proof is due to the author.

We can in fact use Theorem6 to prove that there are infinitely many primes. Although there are already proofs about the infinitude of primes without using the concept of Fermat numbers, it is interesting and worthwhile to see an alternative proof.

Corollary6. [Reference3] There are infinitely many primes.

Proof. Define a sequence $\{pi\}$ in the following way:

i) if F_i is a prime, then define $p_i = F_i$;

ii) if F_i is a composite, then define p_i = a prime factor of F_i.

All the p_i's are distinct by Theorem6. Hence, the set $\{p_i : i = 1, 2, 3 \ldots\}$ contains infinitely many primes. □

Theorem7. [Reference1, p.29] No Fermat number F_n for $n \geq 2$ can be expressed as the sum of two primes.

Proof. Assume for contradiction that there exists $n \geq 2$ such that F_n could be expressed as the sum of two primes. Since F_n is odd, one of the primes must be 2. Then the other prime would equal $F_n - 2 = 2^{2^n} - 1 = (2^{2^{n-1}} + 1)\cdot(2^{2^{n-1}} - 1)$, which is not a prime. □

6 Primality of Fermat Numbers

Recall that we have defined Fermat numbers to be numbers in the form of $2^{2^n} + 1$ where n is a nonnegative integer. There is actually another definition for Fermat numbers, namely numbers in the form of $2^n + 1$ where n is a nonnegative integer. We have chosen the former definition because it seems to be more commonly used and it gives the properties that we have proved earlier. Notice that Theorem6 is false if we had chosen the other definition. A counterexample is $2^1 + 1 = 3$ and $2^3 + 1 = 9$ have a common factor 3.

However, if we are only interested in Fermat numbers that are primes, then it does not matter which definition we use, as we will see from the next theorem.

Theorem8. [Reference3] If $2^n + 1$ is a prime, then n is a power of 2.

Proof. Suppose n is a positive integer that is not a power of 2. Then we can write $n = 2^r \cdot s$ for some nonnegative integer r and some positive odd integer s. Also recall the identity

$$a^n - b^n = (a - b)\cdot(a^{n-1} + a^{n-2}b + \cdots + ab^{n-1} + b^{n-1}),$$

which implies that $a - b$ divides $a^n - b^n$. Now substituting $a = 2^r$, $b = -1$ and $n = s$, we have $2^r + 1$ divides $2^{rs} - (-1)^s = 2^n + 1$. However, $r < n$, which means that $2^n + 1$ is not a prime. Hence, n must be a power of 2 in order for $2^n + 1$ to be a prime. □

The next two theorems concern the properties of Fermat primes.

Theorem9. [Reference1, p. 31] No Fermat prime can be expressed as the difference of two pth powers, where p is an odd prime.

Proof. Assume for contradiction that there is such a Fermat prime. Then, $F_n = a^p - b^p$ $= (a - b)\cdot(a^{p-1} + a^{p-2}b + \cdots + ab^{p-1} + b^{p-1})$, where $a > b$ and p is an odd prime. Since F_n is a prime, it must be the case that $a - b = 1$. Moreover, by Fermat's Little Theorem, $a^p \equiv a \pmod p$ and $b^p \equiv b \pmod p$. Thus, $F_n = a^p - b^p \equiv a - b = 1 \pmod p$. This implies $p \mid F_n - 1 = 2^{2^n}$, which is impossible because the only integer that divides 2^{2^n} is 2. □

Theorem10. [Reference1, p.30] The set of all quadratic nonresidues of a Fermat prime is equal to the set of all its primitive roots.

Proof. First let a be a quadratic nonresidue of the Fermat prime F_n and let $e = \text{ord}_{F_n}a.$ According to Fermat's little theorem, $a^{(F_n - 1)} \equiv 1$ (mod F_n), so $e \mid F_n - 1 = 2^{2^n}$. It follows that $e = 2^k$ for some nonnegative integer $k \le 2^n$. On the other hand, by Euler's criterion, $a^{(F_n-1)/2} = a^{2^{2^n-1}}$

$\equiv -1$(mod F_n). Hence, if $k < 2^n$, then $2^k \mid 2^{2^n-1}$ and so $a^{2^{2^n-1}} \equiv 1$ (mod F_n), which is a contradiction. So, $k = 2^n$ and $\text{ord}_{F_n}a = 2^{2^n}$. Therefore, a is a primitive root modulo F_n.

Conversely, suppose r is a primitive root modulo F_n. It follows that $r^{(F_n - 1)/2} \not\equiv 1$ (mod F_n), and so by Euler's criterion, r cannot be a quadratic residue. □

Now recall that Fermat's little theorem can be used to test whether a number is a prime or not. However, it does not work for Fermat numbers if we choose the base to be 2, as we will see in Theorem11.

Lemma11. [Reference1, p.36] For $m \le 2^n - 1$, $F_m \mid 2^{F_n} - 2$.

Proof. $2^{F_n} - 2 = 2(2^{F_{n-1}} - 1) = 2(2^{2^{2^n}} + 1 - 2) = 2(F_{2^n} - 2) = 2F_0 \cdots F_{2^n - 1}$ (Theorem2). □

Theorem11. [Reference1, p.36] All Fermat numbers are primes or pseudoprimes to base 2. Moreover, if $2^n + 1$ is a pseudoprime to the base 2, then n is a power of 2.

Proof. Since $n \le 2^n - 1$, from Lemma11, $F_n \mid 2^{F_n} - 2$. Since $F_n \neq 2$, we have $F_n \mid 2^{F_{n-1}} - 1$, which is equivalent to say that $2^{F_{n-1}} \equiv 1$ (mod F_n).

Now suppose $2^n + 1$ is a pseudoprime to the base. Then we have $2^{2^n} \equiv 1$ (mod $2^n + 1$). Notice that $2^n \equiv -1$ (mod $2^n + 1$), so $2^{2n} \equiv 1$ (mod $2^n + 1$). Now let $e = ord_{2^n+1}(2)$. First $e \ge n + 1$ for otherwise we will have $2^e \le 2^n < 2^n + 1$. Moreover, $e \mid 2n$, so it follows that $e = 2n$. But $e \mid 2^{2^n}$, which is only possible if n is a power of 2. □

Theorem11 is not true, however, for other bases in general. For examples, F_5 = 4294967297 is not a pseudoprime to base 5 or 6, since we have $5^{4294967296} \equiv$ 2179108346 (mod 4294967297) and $6^{4294967296} \equiv$ 3029026160 (mod 4294967297). Hence, it is still possible to use Fermat's little theorem to test the primality of a Fermat number as long as we do not choose 2 to be our base.

Other than Fermat's little theorem, there are various other primality tests that can be used to test whether a Fermat number (or any number in general) is a prime or not. In the rest of this section, we will discuss in particular two of them. The first one is called Selfridge's test (Theorem13), and the second one is a generalized version of Pepin's test (Theorem14). The proof for the latter involves the use of the Jacobi symbol, which we will introduce here.

Definition. [Reference1, p.25] Let a be an integer and suppose $n \geq 3$ is an odd integer. Write $n = p_1 \cdot p_2 \cdots p_r$, where the p_i's are odd primes but not necessarily distinct. Then the ***Jacobi symbol*** $\left(\frac{a}{n}\right)$ is defined by $\left(\frac{a}{n}\right) = \prod_1^r \left(\frac{a}{p_i}\right)$, where $\left(\frac{a}{p_i}\right)$ is the Legendre symbol.

The Jacobi symbol has properties very similar to those of the Legendre symbol. We state six of them in the following theorem. To familiarize ourselves with the Jacobi symbol, we will prove two of the properties stated. The reader should verify the rest himself. They can be proved using the properties of the Legendre symbol.

Theorem12. [Reference1, p.25] Let $m > 1$ and $n > 1$ be odd integers and let a and b be integers. Then we have the following:

i) if $a \equiv b \pmod{n}$, then $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$;

ii) $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{ab}{n}\right)$;

iii) $\left(\frac{a}{mn}\right) = \left(\frac{a}{n}\right)\left(\frac{a}{m}\right)$;

iv) $\left(\frac{1}{n}\right) = 1$, $\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}$;

v) $\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}$;

vi) $\left(\frac{m}{n}\right) = (-1)^{(m-1)(n-1)/4}\left(\frac{n}{m}\right)$.

Proof[8]***.*** Unless specified, all the $\left(-\right)$ in this proof represent the Legendre symbol.

i) If $a \equiv b \pmod{n}$, then $a \equiv b \pmod{p_i}$ for all prime factors p_i of n. Hence, $\left(\frac{a}{p_i}\right) = \left(\frac{b}{p_i}\right)$ for all p_i's and $\prod_1^r \left(\frac{a}{p_i}\right) = \prod_1^r \left(\frac{b}{p_i}\right)$. Thus, the Jacobi symbols $\left(\frac{a}{n}\right)$ and $\left(\frac{b}{n}\right)$; are equal. □

ii) The Jacobi symbol $\left(\frac{ab}{n}\right) = \prod_1^r \left(\frac{ab}{p_i}\right) = \prod_1^r \left(\frac{a}{p_i}\right)\left(\frac{b}{p_i}\right) = \prod_1^r \left(\frac{a}{p_i}\right) \prod_1^r \left(\frac{b}{p_i}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$, where $\left(\frac{a}{n}\right)$ and $\left(\frac{b}{n}\right)$ are the Jacobi symbols. □

Theorem13. [Reference1, p.42] Let $N > 1$ and let the prime-power factorization of $N - 1$ be $\prod_1^r {p_i}^{k_i}$. Then N is a prime if and only if for each prime p_i where $i = 1, 2, \ldots, r$, there exists an integer $a_i > 1$ such that $a_i^{N-1} \equiv 1 \pmod{N}$ and $a_i^{(N-1)/p_i} \not\equiv 1 \pmod{N}$.

Proof. If N is a prime, then there exists a primitive root a that satisfies both conditions.

Conversely, it suffices to show that $\Phi(N) = N - 1$. Let $e_i = \mathrm{ord}_N a_i$. Then $e_i \mid N - 1$ but $e_i \nmid (N - 1)/p_i$. Hence, $p_i^{k_i} \mid e_i$. We also have $a_i^{\Phi(N)} \equiv 1 \pmod{N}$ by Euler's theorem, so $e_i \mid \Phi(N)$. Consequently, $p_i^{k_i} \mid \Phi(N)$ for all $i = 1, 2, \ldots, r$, and hence, $N - 1 \mid \Phi(N)$. But $\Phi(N) \leq N - 1$, so $\Phi(N) = N - 1$. □

[8] Proof is due to the author.

Theorem14. [Reference1, p.42] For $n \geq 2$, the Fermat number F_n is prime if and only if $a^{(F_n - 1)/2} \equiv -1 \pmod{F_n}$, where a is an integer such that the Jacobi symbol $\left(\frac{a}{F_n}\right) = -1$ for all $n \geq 2$.

Proof. First assume that F_n is prime. Then the Jacobi symbol $\left(\frac{a}{F_n}\right)$ is just the Legendre symbol. So by Euler's criterion, $a^{(F_n - 1)/2} \equiv \left(\frac{a}{F_n}\right) \equiv -1 \pmod{F_n}$.

Now assume that the congruence holds. Then we have both $a^{(F_n - 1)/2} \equiv -1 \pmod{F_n}$ and $a^{(F_n - 1)} \equiv 1 \pmod{F_n}$. Since 2 is the only prime factor of $F_n - 1$, by Theorem13, F_n is a prime. □

Corollary14. [Reference1, p.42] For $n \geq 2$, the Fermat number F_n is prime if and only if $3^{(F_n - 1)/2} \equiv -1 \pmod{F_n}$.

Proof. It suffices to show that $\left(\frac{3}{F_n}\right) = -1$. From Corollary2.1, $F_n \equiv 2 \pmod 3$. Moreover, since $F_n \equiv 1 \pmod 4$, by Theorem12, $\left(\frac{3}{F_n}\right) = (-1)^{(3-1)(4k+1-1)/4}\left(\frac{F_n}{3}\right) = \left(\frac{F_n}{3}\right) = \left(\frac{2}{3}\right) = -1$. □

7 Mersenne Numbers and Fermat Numbers

Recall that we have defined Mersenne numbers to be numbers of the form $2^n - 1$ where n is a positive integer. Some definitions require n to be a prime. However, like the case of Fermat numbers, if we are only interested in Mersenne numbers that are primes, then it does not matter which definition we choose. We can see that in the following theorem.

Theorem15. [Reference4] A Mersenne number $M_n = 2^n - 1$ is prime only if n is a prime.
Proof. Recall the identity $2^{ab} - 1 = (2^a - 1)\cdot(1 + 2^a + 2^{2a} + \cdots + 2^{(b-1)a})$. Hence if $n = ab$ is not a prime, then $M_n = 2^n - 1$ is divisible by $2^a - 1 \neq 1$. □

The next two theorems show how Mersenne numbers relate to the primality of the associated Fermat numbers.

Lemma16. [Reference1, p.44] If p is a prime, then all Mersenne numbers M_p are prime or pseudoprimes to the base 2.
Proof. Let $M_p = 2^p - 1$ be a Mersenne number where p is a prime. If M_p is a composite, then p is odd. By Fermat's little theorem, $(M_p - 1)/2 = 2^{p-1} - 1 \equiv 0 \pmod{p}$. So $(M_p - 1)/2 = kp$ for some positive integer k. Hence, $M_p = 2^p - 1 \mid 2^{kp} - 1 = 2^{(M_p - 1)/2} - 1$. It is equivalent to say that $2^{(M_p - 1)/2} \equiv 1 \pmod{M_p}$, which implies that $2^{M_p - 1} \equiv 1 \pmod{M_p}$. □

Theorem16. [Reference1, p.45] Let p be a prime such that $p \equiv 3 \pmod{4}$. Then the Fermat number F_p is prime if and only if ${M_p}^{(F_p - 1)/2} \equiv -1 \pmod{F_p}$, where M_p is the associated Mersenne number.

Proof. By Theorem14, it suffices to show that $\left(\frac{M_p}{F_p}\right) = -1$.

By Lemma16, $2^{2^p-2} \equiv 1 \pmod{M_p}$, and multiplying 2 to both sides we get $2^{2^p-1} \equiv 2 \pmod{M_p}$. This implies that $F_p = 2\cdot 2^{2^p-1} + 1 \equiv 5 \pmod{M_p}$. Moreover, since $p \equiv 3 \pmod{4}$, $M_p = 2^p - 1 = 2^{4k+3} - 1 = 8\cdot 2^{4k} - 1 \equiv 3\cdot 1 - 1 = 2 \pmod{5}$. Thus, by Theorem 12, $\left(\frac{M_p}{F_p}\right) = \left(\frac{F_p}{M_p}\right) = \left(\frac{5}{M_p}\right) = \left(\frac{M_p}{5}\right) = \left(\frac{2}{5}\right) = -1$. □

Theorem17. [Reference1, p.45] Let p be a prime such that $p \equiv 3$ or 5 (mod 8). Then the Fermat number F_p is prime if and only if $M_p^{(F_{p+1}-1)/2} \equiv -1 \pmod{F_{p+1}}$, where M_p is the associated Mersenne number.

Proof. Again by Theorem14, it sufficies to show that $\left(\frac{M_p}{F_{p+1}}\right) = -1$.

By the same argument in Theorem16, we can show that $F_p \equiv 5 \pmod{M_p}$. Then by Theorem1, $F_{p+1} = (F_p - 1)^2 + 1 = 4^2 + 1 = 17 \pmod{M_p}$. First we assume $p \equiv 3 \pmod 8$, then $M_p = 2^{8k+3} - 1 = 8{\cdot}16^{2k} - 1 \equiv 8 - 1 = 7 \pmod{17}$. Hence, $\left(\frac{M_p}{F_{p+1}}\right) = \left(\frac{F_{p+1}}{M_p}\right) = \left(\frac{17}{M_p}\right) = \left(\frac{M_p}{17}\right) = \left(\frac{7}{17}\right) = -1$.

Now if we assume $p \equiv 5 \pmod 8$, then $M_p = 2^{8k+5} - 1 \equiv 2^5 - 1 = -3 \equiv 14 \pmod{17}$. Hence, $\left(\frac{M_p}{F_{p+1}}\right) = \left(\frac{M_p}{17}\right) = \left(\frac{14}{17}\right) = -1$. □

8 Infinitude of Fermat Primes

As we have noted before, there are only five known Fermat primes so far. In fact, it has been shown that F_n is composite for $5 \leq n \leq 32$ and many other larger n (from section4). Whether there is an infinite number of Fermat primes is still an open question, and below shows a heuristic argument that suggests there is only a finite number of them. This argument is to due to Hardy and Wright [Reference1, p.158].

There is only a finite number of Fermat primes.

Recall that the Prime Number Theorem says $\pi(x) \sim \frac{x}{logx}$, where $\pi(x)$ is the number of primes $\leq x$.

Hence $\pi(x) < \frac{Ax}{logx}$ for some constant A, and the probability that x is a prime is at most $\frac{A}{logx}$.

For $x = 2^{2^n} + 1$, the probability that it is a prime is $\leq \frac{A}{\log{(2^{2^n}+1)}} \leq \frac{A}{log2^{2^n}} = \frac{A}{2^n logx} \leq \frac{A}{2^n}$.

Hence, the expected number of primes in this form is $\leq \sum_0^\infty \frac{A}{2^n} = 2\text{A}$ which is a finite number.

We can use the same reasoning to argue that there are infinitely many twin primes.

There are infinitely many twin primes.

Recall the Prime Number Theorem can be stated using limit: $\lim_\infty \frac{\pi(x)}{x/logx}$.

Hence give $\varepsilon > 0$, there exists a number X such that $1 - \varepsilon < \frac{\pi(x)}{x/logx}$ for all $x > \text{X}$.

Thus, the probability that n and n+2 are both primes is

$$\frac{\pi(n)}{n} \cdot \frac{\pi(n+2)}{n+2} > \frac{1}{logn} \cdot \frac{1}{\log(n+2)} (1-\varepsilon)^2 > \frac{1}{n}(1-\varepsilon)^2 \text{ for } n > \text{X}.$$

So the expected number of twin primes is $> \sum_0^m \frac{1}{n}(1-\varepsilon)^2 + \sum_m^\infty \frac{1}{n}(1-\varepsilon)^2$ which diverges.

However, we must be careful that there two arguments do not prove that there are really only finitely many Fermat primes or infinitely many twin primes. After all, they are only heuristic, as we can see in a similar argument below.

There are infinitely many primes in the form of $2^n + 1$.

Using the exact same argument as above, the expected number of primes in this form is

$> \sum_0^m \frac{1}{logn}(1-\varepsilon)^2 + \sum_m^\infty \frac{1}{logn}(1-\varepsilon)^2$ which diverges.

But we know from Theorem8 that the sets $\{2^n + 1$: it is a prime$\}$ and $\{2^{2^n} + 1$: it is a prime$\}$ are the same set. This latter argument suggests Hardy and Wright's argument does not take into account of the properties of Fermat numbers. It is to say that the variable x is not that random. It works largely because gaps between successive Fermat numbers are extremely large.

Nevertheless, given any number (even a number of a particular form), it is more likely to be a composite than prime. Therefore, bounding the probability of it being a prime by a lower bound gives a weaker argument that bounding it from above.

9 Divisibility of Fermat Numbers

In the last two sections, we focused on the primality of Fermat numbers and the properties of Fermat primes. However, if a Fermat number is found to be composite, we are interested in what its factorization is, or at least, what properties do its divisors have to have. We will end our discussion of Fermat numbers in this section by proving several theorems about their divisors.

Theorem 18. [Reference1, p.37] Let $q = p^m$ be a power of an odd prime p, where $m \geq 1$. Then the Fermat number F_n is divisible by q if and only if $\text{ord}_q 2 = 2^{n+1}$.

Proof. First suppose $q \mid F_n$, then $q \mid (2^{2^n} + 1)\cdot(2^{2^n} - 1) = 2^{2^{n+1}} - 1$, and hence $2^{2^{n+1}} \equiv 1 \pmod{q}$. It follows that $2^{n+1} = k\text{ord}_q 2$ for some positive integer k. Thus, k is a power of 2 and so is $\text{ord}_q 2$. Let $e = \text{ord}_q 2 = 2^j$. If $j < n + 1$, then we have $q \mid 2^{e2^{n-j}} - 1 = 2^{2^n} - 1$. But this is impossible because $q \mid 2^{2^n} + 1$ and $q \neq 2$. Hence, $j = n + 1$ and so $\text{ord}_q 2 = 2^{n+1}$.

Conversely, if we assume that $\text{ord}_q 2 = 2^{n+1}$, then $q \mid 2^{2^{n+1}} - 1 = (2^{2^n} + 1)\cdot(2^{2^n} - 1)$. Since q is an odd prime, q divides either $2^{2^n} + 1$ or $2^{2^n} - 1$. But q cannot divide $2^{2^n} - 1$ because $2^n < \text{ord}_q 2$. Hence $q \mid 2^{2^n} + 1 = F_n$. □

Theorem19(Euler). [Reference1, p. 38] If p is a prime and $p \mid F_n$, then p is of the form $p = k2^{n+1} + 1$, where k is a positive integer.

Proof. By Fermat's little theorem, $2^{p-1} \equiv 1 \pmod{p}$, and it follows that $\text{ord}_q 2 \mid p - 1$. Hence, $k\ \text{ord}_q 2 = p - 1$ for some positive integer k, and by Theorem18, $p = k\text{ord}_q 2 + 1 = k2^{n+1} + 1$. □

Theorem20(Lucas). [Reference1, p.59] If $n > 1$ and a prime p divides F_n, then p is of the form $p = k2^{n+2} + 1$, where k is a positive integer.

Proof. Let $b = 2^{2^{n-2}} (2^{2^{n-1}} – 1)$. Since $p \mid F_n = 2^{2^n} + 1$, we have $2^{2^n} \equiv –1 \pmod p$. Hence, $b^2 = 2^{2^{n-1}} (2^{2^n} – 2{\cdot}2^{2^{n-1}} + 1) \equiv 2^{2^{n-1}} (–1 – 2{\cdot}2^{2^{n-1}} + 1) = –2{\cdot}2^{2^n} \equiv 2 \pmod p$. It then follows that $b^{2^{n+1}} = 2^{2^n} \equiv –1 \pmod p$ and thus $b^{2^{n+2}} \equiv 1 \pmod p$. Consequently, $e = \mathrm{ord}_p b = 2^j$ for some $j \le n + 2$. If $j < n + 2$, then $b^{e2^{n+1-j}} – 1 = b^{2^{n+1}} – 1 \equiv 2^{2^n} – 1 \equiv 0 \pmod p$. This contradicts to the previous result that $2^{2^n} + 1 \equiv 0 \pmod p$. Hence, $j = n + 1$ and $\mathrm{ord}_p b = 2^{n+2}$.

Now since $b^2 \equiv 2 \pmod p$, it follows that $\gcd(b, p) =1$. By Fermat's little theorem, $b^{p-1} \equiv 1 \pmod p$. Thus, $\mathrm{ord}_p b = 2^{n+2} \mid p – 1$, and hence $p = k2^{n+2} + 1$ for some positive integer k. □

Corollary20. [Reference1, p.39] If $n > 1$, then any divisor $d > 1$ of a Fermat number F_n is of the form $k2^{n+2} + 1$, where k is a positive integer.

Proof. Consider the product $(k2^{n+2} + 1){\cdot}(k2^{m+2} + 1)$. Without loss of generality, assume $m \ge n$. Then $(k2^{n+2} + 1){\cdot}(k2^{m+2} + 1) = k^2 2^{m+n+4} + k2^{n+2} + k2^{m+2} + 1 = (k^2 2^{m+2} + k + k2^{m-n})2^{n+2}$, which is also in the form of $k2^{n+2} + 1$. Following from Theorem19, all divisors have the form $k2^{n+2} + 1$. □

10 References

1. M. Krizek, F. Luca and L. Somer, *17 Lectures on Fermat Numbers – From Number Theory to Geometry*, Springer-Verlag, New York, 2001.

2. W. Keller, *Prime factors* $k{\cdot}2^n + 1$ *of Fermat numbers* F_m *and complete factoring status.* http://www.prothsearch.net/fermat.html#Summary

3. _____, *Fermat number* http://en.wikipedia.org/wiki/Fermat_numbers

4. _____, *Mersenne number* http://en.wikipedia.org/wiki/Mersenne_numbers