Primality of the Fermat Number F_5

Jeyram Ananda Krishnan

August 2023

1 Fermat Numbers

In order to decipher the primality of a Fermat number, we must define the form in which a number must fit in order to be classified as such.

Definition 1.1 (Fermat Numbers)**.** Fermat numbers are positive integers of the form $F_n = 2^{2^n} + 1$.

Fermat had claimed that all numbers of this form were prime as $2^{2^0} = 2 + 1 = 3$, $2^{2^1} = 4 + 1 = 5$, $2^{2^2} = 16 + 1 = 17$, $2^{2^3} = 256 + 1 = 257$, $2^{2^4} = 65536 + 1 = 65537$, the first five Fermat numbers, are prime. Perhaps it was the glaring incompleteness behind Fermat's conclusion in proving that this pattern would hold for all $n \in \mathbb{Z}_{\geq 0}$, the set of all nonnegative integers, that led Euler to attempt to determine the primality of F_5.

2 Numbers of the Form $a^n + 1$

Numbers of the form $a^n + 1$, where $n \in \mathbb{Z}_{\geq 0}$ and a is any number, always has divisors the following condition:

$a^{2m+1} + 1$ can be divided by a + 1 and $a^{p(2m+1)} + 1$ by $a^p + 1$ for any number substituted in place of a.

Proof. $a^{2m+1} + 1$ can be written in the form

$$(a + 1)(a^{2m} - a^{2m-1} - a^{2m-2} - ... - a + 1)\forall m \in \mathbb{Z}_{\geq 0},$$

meaning that $(a+1)|(a^{2m+1})$. Similarly, $a^{p(2m+1)}+1$ can be written in the form

$$(a^p + 1)(a^{p(2m)} - a^{p(2m-1))} - a^{p(2m-2)} - ... - a^p + 1)\forall m \in \mathbb{Z}_{\geq 0},$$

meaning that $(a^p + 1)|(a^{p(2m+1)})$.

□

As a result of the proof of (1), which accounts for all values of n such that $n = 2m + 1$ or $n = p(2m + 1)$, that is, n is a number with any odd factors, or not a power of two, we can turn our attention to numbers in the form $a^{2^n} + 1$, a case that closely resembles the Fermat number F_n When looking at a number of the form $a^{2^m} + 1$, we can see that it would be included in the set of numbers for which the previous condition would apply. However, it cannot be concluded that the primality $a^{2^m} + 1$ can be generalized over all numerical values of a simply due to numbers of the form $a^n + 1$ holding the listed properties over all such values.

Clearly, if a is an odd integer, then the resulting number $a^{2^m} + 1$ would have an even parity(and would be composite as a result) regardless of the numerical value of m on account of a^{2^m} being an odd integer.

Even if a is even, there exists an infinite number of examples of cases in which $a^{2^m} + 1$ is indeed composite.

For example, when $m = 1$, that is, when the number is in the form $a^2 + 1$, it is composite for any value of a that can be represented in the form $5b \pm 3$, where $b \in \mathbb{Z}_{>0}$, as any number generated under such conditions, such as 50, 65, 145, 170, are all multiples of 5. Other cases under which $a^2 + 1$ include when $a = 30$ and $a = 50$, when the numbers produced are divisible by 17 and 41, respectively.

Composite values for cases in which $n \neq 1$ also exist, including $10^4 + 1$, $6^8 + 1$, and $6^{128} + 1$, which are divisible by 73, 17 and 257, respectively.

Although composite numbers of the form $a^{2^m} + 1$ can be found, Fermat could not find any composite numbers of the form $2^{2^m} + 1$, since, at the time, the table of primes extended to 100000. Therefore, as the first five Fermat numbers were primes, and perhaps with the examples of composite cases of $a^n + 1$, where a is even, being as scarce as they are, Fermat came to the premature conclusion that all numbers of such a form would be prime. However, as Euler showed, this is not the case.

3 Primality of F_5

When examining the case of the Fermat number, Euler picked up where Fermat left off, starting with examining the primality of the Fermat number where $n = 5$.

$$F_5 = 2^{2^5} + 1 = 2^{32} + 1 = 4294967297$$

Euler observed that this number is divisible by 641, thus proving that the method which Fermat used to compute a prime greater than any given number was false.

4 Numbers of the Form $a^n - 1$

Numbers of the form $2^n - 1$, and more generally, numbers of the form $a^n - 1$, is composite whenever n is not prime.

Proof. Let us assume that numbers of the form $a^n - 1$, where $a \in \mathbb{Z}_{>0}$, a and n are greater than 1, are prime. Such numbers can be expressed in the following form:

$$a^n - 1 = (a - 1)(a^{n-1} + a^{n-2} + ... + a + 1)$$

From this, we can see that $(a - 1)|(a^n - 1)$.

However, since $a^n - 1$ is prime, and $a - 1 = 1$ or $a - 1 = a^n - 1$ as a result(with the latter being impossible as $n > 1$, then $a = 2$. Therefore, we can establish that if $a^n - 1$ were to be prime, then the value of a must be 2.

We can set $n = bc$, where $b, c \in \mathbb{Z}_{>0}$, b and c are greater than 1, and they are both less than n. Then

$$a^{bc} - 1 = (a^b - 1)(a^{b(c-1)} + a^{b(c-2)} + ... + a^b + 1)$$

Therefore, we can say that $(a^b - 1)|(a^{bc} - 1)$, meaning that a number of the form $a^{bc} - 1 = a^n - 1$, which we have narrowed down to $2^n - 1$, must be composite. □

While we have proved that if n is not prime, that $2^n - 1$ should be composite, we have not done so with the converse, in that $2^n - 1$ must be prime in the case that n is prime.

This notion can be refuted simply with the counterexample given by Euler, in that $2^{11} - 1 = 2047$ has divisors 23 and 89, therefore putting to rest the possibility that $2^n - 1$ is always prime, and again not allowing for there to be such a simple method to compute a prime greater than any given number, as Fermat proposed. Euler sought to find a rule for the exceptions of the cases in which $2^n - 1$, where n is prime, is a prime number, that is, the cases in which a number of the form is not so.

For example, when looking at the cases in which n can be written in the forms $n = 4m - 1$ and $n = 8m - 1$, where $m \in \mathbb{Z}_{>0}$, for which the resulting number $a^n - 1$ is always divisible by $8m - 1$. This results in the exclusion of the following possible values of n: 11, 23, 83, 131, 179, 191, 239, and so on for all prime values of n that can be written in the forms $4m - 1$ and $8m - 1$.

Despite these restrictions, there continue to be numerous cases in which $a^n - 1$ is composite, including $2^{37} - 1$, which is divisible by 223, $2^{43} - 1$, which is divisible by 431, and so on.

5 Divisibility of $a^n - b^n$

Euler asserted that numbers of the form $a^n - b^n$, where $a, b, n \in \mathbb{Z}_{>0}$ and $n > 1$, are divisible by $n + 1$ if $n + 1$ is any prime number that neither divides a nor b. He did not provide proof for this, citing the primality of $n+1$ as a reason as to why this could serve to be difficult. Nevertheless, we can analyze the results of this proposition if it were to, indeed, be true. Some of its results are the following:

$$(n + 1)|(2^n - 1)$$

if n+1 is prime, and

$$(2m + 1|(2^{2m} - 1)$$

if $2m+1$ is a prime number. This can be directly followed by the previous result as all prime numbers(other than two, which is not allowed by the proposition), are odd.

From the previous statement, we can conclude that either $2^n + 1$ or $2^n - 1$ can be divided by $2n + 1$, since $2^{2n} - 1 = (2^n + 1)(2^n - 1)$.

Euler states a multitude of other theorems as a result of his finding that $(n + 1)|(a^n - b^n)$ if $n+1$ is prime, but we will narrow our discussion to on in particular and its similarity to another well-known theorem.

6 Fermat's Little Theorem

Euler states the following as a result of his discussion of the divisibility of $a^n - b^n$:

If n is a prime number, all powers having the exponent $n-1$ leave either nothing or 1 when divided by n.

This closely resembles Fermat's little theorem, which states the following:

Theorem 1 (Fermat's Little Theorem)**.** *If n is prime,* $a^n \equiv a(mod\ n)\ \forall a \in \mathbb{Z}$.

The following lemma will be used in the proof of this theorem.

Lemma 1. *For all x,* $y \in \mathbb{Z}$ *and prime n,* $(x + y)^n \equiv x^n + y^n(mod\ n)$.

Proof. This lemma is also known as the freshman's dream. Starting the proof with considering the binomial expansion of $(x + y)^n$, paying close attention to the behavior of the coefficients.

$$(x + y)^n = \sum_{k=0}^{\infty} \binom{n}{k} x^k y^{n-k}$$

The binomial coefficients can be written in the following form

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

Examining this, considering that $0 < k < n$, we can see that the denominator of the right-hand side expression has no prime factors of n, as n is prime. Therefore, we can say that

$$\binom{n}{k} \equiv 0 \pmod{n}$$

The condition that $0 < k < n$ applies all terms with the exception of the resulting polynomial's initial and final terms, these being x^n and y^n. We can now say that

$$(x + y)^n \equiv x^n + y^n \pmod{n}$$

□

Proof of Theorem 1. We can prove Fermat's Little Theorem for all $a \in \mathbb{Z}_{\geq 0}$ using mathematical induction. We can first test the base case, which is

$$0^n \equiv n \pmod{n}$$

We can now assume that the statement holds for some $a \in \mathbb{Z}_{\geq 0}$, or that $a^n \equiv n \pmod{n}$, and resume with our inductive step using the freshman's dream lemma. From this, we get

$$(a + 1)^n \equiv a^n + 1 \pmod{n}$$

This is Fermat's Little Theorem for $a + 1$, so the theorem has been proved. □

7 Infinitely Many Primes

Fermat, after coming to the conclusion that 2^{2^n} is prime for any integer, believed that this gave a way to compute the value of a prime number greater than any given number in a relatively simple manner. While there is still no formula from which we can reliably construct primes greater than any given number, we can prove that there ought to be so in the first place using the following theorem, which is provided by Euclid.

Theorem 2 (Euclid's Theorem)**.** *There are infinitely many prime numbers.*

Proof. Assume that there exists a last prime number p_n be the nth prime number, if all prime numbers were to be arranged in ascending order. Now let

$$P = p_1 p_2 p_3 \cdots p_n + 1$$

Since $P > 1$ and by our original assumption, P must be composite, it should be divisible by some prime p, that is, one number in the sequence $p_1 p_2 p_3 ... p_n$. Since $p|(p_1 p_2 p_3 ... p_n)$ and $p|P$, we can conclude that $p|(P - (p_1 p_2 p_3 ... p_n))$. Therefore, $p|1$. From this, we can see that the only possible value of p is 1 in this case. However, $p > 1$, and we can conclude that for our original assumption was false, and that for any finite set of prime numbers, there exists a prime not in this set, that is, that there are infinitely many prime numbers. Thus, for any given number, there exists a prime greater than the given number. While there still exists no simply way to compute such numbers, there are limits that can be set on the value of a hypothetical nth prime number, such as $2^{2^{n-1}}$, or Fermat's nth number, which is the greatest possible value of the nth prime number. □

References

[1] David Burton (2010) *Elementary Number Theory*, McGraw Hill Education

[2] Leonhard Euler(1738) *Observationes de theoremate quodam Fermatiano alisque ad numeros primos spectantibus*, Commentarii academiae scientiarum Petropolitanae, Volume 6, pp. 103-107.