Theoretical Mathematics & Applications, vol.6, no.1, 2016, 15-37
ISSN: 1792-9687 (print), 1792-9709 (online)
Scienpress Ltd, 2016

The $n^2 + 1$ Fermat and Mersenne prime numbers conjectures are resolved

Robert Deloin[1]

Abstract

In 1912 in Cambridge, the fourth problem mentioned by Landau in the Fifth Congress of Mathematicians was the conjecture that there are infinitely many primes p of the form $p = n^2 + 1$.

In 1640, the French mathematician Fermat conjectured that all numbers $F_n = 2^{2^n} + 1$ were prime. Today, this conjecture has become that there are no Fermat prime numbers greater than $F_4 = 2^{2^4} + 1 = 65537$.

In 1644, the French Minim Friar Marin Mersenne conjectured that the function $f_n = 2^n - 1$ generates prime numbers only for n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127 and 257. Today, we know that this is wrong for 67 and 257 and that 48 Mersenne prime numbers exist. The conjecture is now that there are infinitely many Mersenne prime numbers.

As of 2015, these three conjectures are unresolved.

The main contribution of this paper is to introduce a new approach to these questions. The key idea of this new approach is that these problems can be solved by a system made of an appropriate test and a congruence with fixed modulus, both dedicated to each kind of number.

[1] No Affiliation. E-mail: rdeloin@free.fr

Article Info: *Received* : August 22, 2015. *Revised* : September 19, 2015.
Published online : January 5, 2016.

Mathematics Subject Classification: 11A07; 11A15; 11A41; 11A51
Keywords: n^2+1; problem; prime; Fermat; Mersenne; conjecture; congruence

1 Introduction

In 1640, in a letter to his friend Frenicle, the French mathematician Pierre de Fermat(1601-1665) conjectured that all numbers $F_n = 2^{2^n} + 1$ were prime. But Fermat did not prove it. Euler, a century later, showed that $F_5 = 2^{2^5} + 1$ is divisible by 641. In 2015, only F_0 to F_4 (3, 5, 17, 257, 65537) are known to be prime, F_5 to F_{32} are known to be composite as well as a lot of disparate other ones and the conjecture about Fermat prime numbers is now that there are no Fermat prime numbers $F_n > F_4$.

In 1644, the French Minim Friar Marin Mersenne (1588-1648) conjectured that the function $f_n = 2^n - 1$ generates prime numbers only for n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127 and 257.

Today, we know that 67 and 257 are wrong and that 61, 89 and 107 have to be added to this list as well as others up to a list of 48 numbers. The conjecture is now that there are infinitely many Mersenne prime numbers.

In 1912, the conjecture that there are infinitely many primes p of the form $p = n^2 + 1$ was still an open problem as mentionned by Landau [1]. As this problem involves a polynomial, the conjecture [2] of the Polish mathematician Bunyakovsky (1804-1889) about the general integer polynomial function is important for its definition of the *indivisibility* of such functions.

2 Preliminary notes

2.1 The composite numbers

According to the fundamental theorem of arithmetics and to the convention that the number 1 is not prime, each composite number N greater than 1 can be factorized in only one way by powers of increasing primes:

$$\mathrm{N} = \prod_i p_i^{\alpha_i}$$

A consequence of it is that any natural number greater than 1 is either a prime (2 or an odd prime) or a multiple qp of any prime p of its factorization.

2.2 The composite values of an integer function

The last section applies to the integer values generated by any indivisible integer polynomial function, the word indivisible being taken with the meaning of Bunyakovsky [2]:

gcd (coefficients of polynomial) = 1,
no fixed divisor divides all values of the function,
the function is irreducible.

We have to notice here that when there exists no formula giving a direct factorization for a given polynomial integer function f(n) of degree m>1 as, by instance, the well known relation n^2-a^2 = (n-a)(n+a), or the aurifeuillean factorization, the only remaining reference for the factorization of each value f_n is the infinite table of factorization of all natural numbers, whose existence is proved by the above cited fundamental theorem of arithmetics, a table that cannot entirely exist due to its infinite dimension but that can be refered to via mathematical softwares dealing with very big numbers.

2.3 A method to isolate prime values of a function

The core of the method is based on the fact that if a statement is true for all the n values in the set of congruences:

$$n = \{1, ..., \mu\} \bmod \mu$$

where μ is an explicit integer number, indeed the statement is true for all natural numbers n, and this set of congruences modulo μ is a covering system of the set $\mathbb{N}$.

So, the practical method will be to search for a maximum of possible congruences for which the statement:

f_n is always divisible by an odd divisor μ_j >1

apply to a function f_n.

These congruences can be of two kinds:

- congruences with a zero residue and a fixed modulus μ_j; as they define *composite* numbers, their number will be named c;

- congruences with a non zero or variable residue and a fixed or variable modulus; as they can contain *prime* numbers, their number will be named p.

As the c disparate congruences with a zero residue cover *composite* values of the function, for a modulus $\mu = lcm(\mu_j)$, they are the solution of the statement:

f_n is always divisible by an odd divisor $\mu_j > 1$

This search for congruences will always end into one of the following three cases:

- c>0 and p=0: if this set of c congruences is a covering system of modulus μ of all the values of the function, all these values are composite and divisible by a finite set of divisors d_j named the covering set of the divisors of the function values, this set being used repeatedly, infinitely many times by the function with the μ period. This is the case of the functions $f_n = R2^n - 1$ and $f_n = S2^n + 1$ using the Riesel (R) and Sierpiński (S) numbers as shown in [3] [4] and used in [5].

- c>0 and p>0: if this set of c+p congruences is a covering system of modulus μ of all the function values with c congruences of modulus μ containing only composite values and p congruences, also of modulus μ, containing infinitely many composite values and according to Dirichlet theorem, infinitely many primes, the function generates infinitely many primes unless a limit exists that prevents it.

- c=0 and p>0: no μ modulus can be found for the set of p congruences. No instance of this case has been encountered so that this case has not been studied here.

3 Proof of n^2+1 prime numbers conjecture

The conjecture to be proved is that the integer function n^2+1 generates infinitely many prime numbers.

3.1 A first set of congruences with fixed modulus

To study the integer function f(n)=n^2+1, we first look at the factorizations of f_n for n varying from 1 to some value that we will take here, by instance, to be 21 (it has to be big enough to be able to show congruences):

Table 1. Factorizations of $f_n=n^2+1$ for n=1,21

Function f	Value	Factorization
$f=1^2+1=$	2	prime
$f=2^2+1=$	5	prime
$f=3^2+1=$	10	$=2\times5$
$f=4^2+1=$	17	prime
$f=5^2+1=$	26	$=2\times13$
$f=6^2+1=$	37	prime
$f=7^2+1=$	50	$=2\times5^2$
$f=8^2+1=$	65	$=5\times13$
$f=9^2+1=$	82	$=2\times41$
$f=10^2+1=$	101	prime
$f=11^2+1=$	122	$=2\times61$
$f=12^2+1=$	145	$=5\times29$
$f=13^2+1=$	170	$=2\times5\times17$
$f=14^2+1=$	197	prime
$f=15^2+1=$	226	$=2\times113$
$f=16^2+1=$	257	prime
$f=17^2+1=$	290	$=2\times5\times29$
$f=18^2+1=$	325	$=5^2\times13$
$f=19^2+1=$	362	$=2\times181$
$f=20^2+1=$	401	prime
$f=21^2+1=$	442	$=2\times13\times17$

from which it can be easily proved, repetitions of numbers being allowed, that

with no limit on n, we have a set of 7 congruences for the composite values of the function f(n)=n^2+1:

$$\text{when n} = 1+2\alpha,\ \text{f}_n \equiv 0 \bmod 2$$
$$\text{when n} = \{2,3,7,8\}+10\alpha,\ \text{f}_n \equiv 0 \bmod 5$$
$$\text{when n} = \{5,8\}+13\alpha,\ \text{f}_n \equiv 0 \bmod 13$$

By instance, to prove the last one for unlimited n=8+13α:

$$\text{f}_n = (8+13\alpha)^2 +1$$
$$\text{f}_n = (13^2\alpha^2 + 2 \times 8 \times 13\alpha + 64) +1$$
$$\text{f}_n = 13^2\alpha^2 + 2 \times 8 \times 13\alpha + 5 \times 13$$
$$\text{f}_n \equiv 0 \bmod 13$$

3.2 A covering system of congruences with fixed modulus

Now, without repetitions and using the least common multiple μ=130 of the moduli 2, 10 and 13 of the above congruences, we see that these congruences cover:

$$\text{n} = \{1,2,3,-,5,-,7,8,9,-,11,12,13,-,15,-,17,18,19,-,...,129,-\} \bmod 130$$
and not:
$$\text{n} = \{4,6,10\} \bmod 10$$

So, for a better understanding of what happens when n = {4,6,10} mod 10, we use only these values in the extended Table 2 which follows.

Table 2. Values of f_n=n^2+1 for n={4,6,10}+10α

Function f	Value	Factorization
f=4^2+1 =	17	prime
f=6^2+1 =	37	prime
f=10^2+1 =	101	prime
f=14^2+1 =	197	prime
f=16^2+1 =	257	prime
f=20^2+1 =	401	prime
f=24^2+1 =	577	prime
f=26^2+1 =	677	prime
f=30^2+1 =	901	= 17×53
f=34^2+1 =	1157	= (13)×89
f=36^2+1 =	1297	prime
f=40^2+1 =	1601	prime
f=44^2+1 =	1937	= (13)×149
f=46^2+1 =	2117	= 29×73
f=50^2+1 =	2501	= 41×61
f=54^2+1 =	2917	prime
f=56^2+1 =	3137	prime
f=60^2+1 =	3601	= (13)×277
f=64^2+1 =	4097	= 17×241
f=66^2+1 =	4357	prime
f=70^2+1 =	4901	= $(13)^2$×29
f=74^2+1 =	5477	prime
f=76^2+1 =	5777	= 53×109
f=80^2+1 =	6401	= 37×173
f=84^2+1 =	7057	prime
f=86^2+1 =	7397	= (13)×569
f=90^2+1 =	8101	prime
f=94^2+1 =	8837	prime
f=96^2+1 =	9217	= (13)×709
f=100^2+1 =	10001	= 73×137

where numbers in parenthesis are already found to be periodical:

when n = 5+13α, n=5,18,31,44,57,70,83,96, $f_n \equiv 0 \bmod 13$

and when n = 8+13α, n=8,21,34,47,60,73,86,99, $f_n \equiv 0 \bmod 13$.

This table shows no congruences with new factors but, about the f_n values, it shows that:

when n={4,6}+10α, $f_n \equiv 7 \bmod 10$ for $n > 3$
when n=10+10α, $f_n \equiv 1 \bmod 10$ for $n > 3$

So:
- when n = {1,2,3,-,5,-,7,8,9,-}+10α we found that f_n is always a multiple of 2, 5 or 13,
- but when n={4,6,10}+10α, we found that f_n cannot be a multiple of a periodical factor.

This proves that this sytem of congruences is a covering system of $\mathbb{N}$ but that the covering set of prime divisors d_j of f_n is infinite due to the presence of the congruences:

when n={4,6}+10α, $f_n \equiv 7 \bmod 10$ for $n > 3$
when n=10+10α, $f_n \equiv 1 \bmod 10$ for $n > 3$

3.3 The appropriate test for general primes

In 1967, improving the tests proved by Lucas in 1876 and 1891, Brillhart and Selfridge [6] have proved the following theorem:

With N>1, it is supposed that for any prime factor q of $N-1$,
there exists an integer c = c(q) > 1 such that:
(i) $c^{N-1} \equiv 1 \mod N$
(ii) $c^{(N-1)/q}$ not $\equiv 1 \mod N$
then, N is prime.

With $N = n^2+1$, this test becomes:

With n> 0, it is supposed that for any prime factor q of n^2,
there exists an integer c = c(q) > 1 such that:
(i) $c^{n^2} \equiv 1 \mod (n^2+1)$
(ii) $c^{(n^2)/q}$ not $\equiv 1 \mod (n^2+1)$
then, n^2+1 is prime.

3.4 Proof of n^2+1 prime numbers conjecture

When n={4,6,10}+10α (always even), we found that for $n > 3$, $f_n \equiv \{1,7\}$ mod 10 cannot be a multiple of a periodical factor.

Now, from all these f_n values, by Eratosthenes' sieve, we keep only those that are prime, whose number is unknown but whose we know that they all verify Brillhart and Selfridge's test.

As all the prime values $f_n > 5$, whose number is unknown, belong to the congruences $f_n \equiv \{1,7\} \mod 10$ for $n > 3$ which, according to Dirichlet' theorem, contain infinitely many primes, this proves that the function $f_n = n^2+1$ generates primes that are solutions of the system of congruences:

$$\text{(i) } c^{n^2} \equiv 1 \mod (n^2+1)$$
$$\text{(ii) } c^{(n^2)/q} \text{ not} \equiv 1 \mod (n^2+1)$$
$$\text{for q=2 or any odd prime factor q of } n^2$$
$$\text{and:}$$
$$n^2+1 \equiv \{1,7\} \text{ mod 10 for } n > 3$$

As $n^2 = f_n - 1$, for the prime values of $f_n = n^2+1$ and according to Fermat's little theorem, relation (i) is always verified if f_n does not divide c.

But the n's that make f_n prime still have to verify relation (ii) of Brillhart and Selfridge's test.

Now, we will prove that (ii) has infinitely many integer solutions n that make n^2+1 prime.

Proof. **Hypothesis** If (ii) has infinitely many integer solutions n that make n^2+1 prime, it means that there exists no limit L beyond which (if $n > L$), $f_n = n^2+1$ is never a prime and (ii) of Brillhart and Selfridge's test is never verified.

As $n = \{4,6,10\} + 10\alpha > L$ is always even, n^2 will always be divisible by 4 so that for $q = 2$, n^2/q will always be even. Let's set: $n^2/2 = 2\alpha$ and we have, using the definition of quadratic residues for prime numbers n^2+1 and Euler's congruence for Legendre's symbol:

$$\left(\frac{c^{n^2/2}}{n^2+1}\right) = \left(\frac{c^{2\alpha}}{n^2+1}\right) = \left(\frac{(c^\alpha)^2}{n^2+1}\right) = 1 \equiv c^{n^2/2} \mod (n^2+1)$$

and (ii) of Brillhart and Selfridge's test will never be verified when q=2, on one hand.

On the other hand, n^2/q is always integer when q is an odd divisor of n. So, if q is any odd divisor of n, we can set $y = n/q$ so that $n^2/q = ny$ and we have:

$$c^{n^2/q} \equiv c^{ny} \mod (n^2+1)$$

As $n = \{4, 6, 10\} + 10\alpha$ is always even, let's set $n = 2\beta$, and we have, using the definition of quadratic residues for prime numbers n^2+1 and Euler's congruence for Legendre's symbol:

$$\left(\frac{c^{n^2/q}}{n^2+1}\right) = \left(\frac{c^{ny}}{n^2+1}\right) = \left(\frac{c^{2\beta y}}{n^2+1}\right) = \left(\frac{(c^{\beta y})^2}{n^2+1}\right) = 1 \equiv c^{n^2/q} \mod (n^2+1)$$

and (ii) of Brillhart and Selfridge's test will never be verified when q is any odd divisor of n.

As we get the impossibility for (ii) of Brillhart and Selfridge's test to be verified when $q = 2$ or any odd divisor of any $n > 3$, we also get the contradiction to our hypothesis that there would exist a limit L beyond which there would be no more n^2+1 primes.

We will now show that this is a wrong contradiction because it does not take into account the fact that the prime values of f_n have to verify $f_n = n^2+1 \equiv \{1, 7\} \mod 10$ or $f_n = \{1, 7\} + 10k$.

As congruence (ii) is:

$$\text{(ii) } c^{(n^2)/q} \text{ not} \equiv 1 \mod (n^2+1)$$

for $k = 10^m$, $f_n = \{1, 7\} + 10k = \{1, 7\} + 10^{m+1}$ and $n^2 = f_n - 1$, we have:

$$\text{(ii) } c^{(\{0,6\}+10^{m+1})/q} \text{ not} \equiv 1 \mod (n^2+1)$$
or, elevating both sides of this congruence at power q:
$$c^{\{0,6\}} c^{10^{m+1}} \text{ not} \equiv 1 \mod (n^2+1)$$

As $f_n > 3$ never divides 3, we can now choose $c = 3$ in Brillhart and Selfridge's test. We have then on one hand, for the left side with a direct calculus:

$$\begin{array}{ccc} \text{As: } 3^0 = 1,\ 3^6 = 729, & & 3^{10} = 59049, \\ \text{and: } 3^{10^m} & \equiv & 1 \mod 10 \text{ for } m > 1 \\ 3^{\{0,6\}+10^{m+1}} & \equiv & \{1,9\} \mod 10 \text{ for } m > 1 \\ 3^{\{0,6\}+10^{m+1}} \mod f_n & \equiv & \{1,9\} \mod 10 \mod f_n \text{ for } m > 1 \\ \text{and, on the other hand,} & & \text{for the right side:} \\ f_n & \equiv & \{1,7\} \mod 10 \\ f_n + 1 & \equiv & \{2,8\} \mod 10 \\ 1 \mod f_n & \equiv & \{2,8\} \mod 10 \mod f_n \end{array}$$

and, as we always have:

$$\{1,9\} \mod 10 \mod f_n \neq \{2,8\} \mod 10 \mod f_n.$$

(ii) is always verified for any $n > 3$.

This proves that no fixed limit L exists beyond which there is no more prime values of $f_n = n^2 + 1 = \{1,7\} \mod 10$ for $n > 3$.

The non-existence of such a limit proves that the function $f_n = n^2 + 1$ generates infinitely many primes. □

In the next section, the existence of a limit will prove that Fermat primes are not infinitely many.

4 Fermat prime numbers conjecture

Fermat prime numbers F_n [7] are the prime numbers generated by the function:

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

4.1 A first set of congruences with fixed moduli

There is an obvious recurrence relation between Fermat numbers:

$$\begin{array}{c} \text{from: } f_{n+1} = 2^{2^{n+1}} + 1 \\ f_{n+1} - 1 = (2^{2^n})^2 \\ f_{n+1} = (f_n - 1)^2 + 1 \end{array}$$

From this relation, we can find the following general relation:

$$\begin{array}{rcc} f_{n+1} & = & f_n^2 - 2f_n + 2 \\ & = & f_n(f_n - 2) + 2 \\ & = & f_n(f_{n-1}(f_{n-1} - 2)) + 2 \\ & = & f_n f_{n-1}(f_{n-2}(f_{n-2} - 2)) + 2 \\ & & \cdots \\ & = & f_n f_{n-1} f_{n-2} ... f_1 f_0 + 2 \\ f_{n+1} & = & 2 + \prod_{k=0}^{n} f_k \end{array}$$

From this relation, the first set of congruences is:

$$f_{n+1} \equiv 2 \mod f_{k=0,n}$$

which proves that all f_n values are relatively prime with all their previous values f_k. Making n tend to infinity, this proves that all f_n values are relatively prime.

4.2 A second set of congruences with variable moduli

As $f_{n+1} = 2 + \prod_{k=0}^{n} f_k$, we also have:

$$f_{n+1} - 2 = \prod_{k=0}^{n} f_k$$
or:
$$f_n - 2 = \prod_{k=0}^{n-1} f_k$$

so that:

$$\frac{f_{n+1} - 2}{f_n - 2} = f_n$$
$$f_{n+1} - 2 = f_n(f_n - 2)$$

hence, the second set of congruences:

$$f_{n+1} \equiv 2 \mod f_n \text{ (already found in the first set)}$$
$$f_{n+1} \equiv 2 \mod (f_n - 2)$$

4.3 A congruence with a fixed modulus

For $f_n > 5$ or n>1 let's set: n=2+k. We thus have:

$$\begin{aligned} f_n &= f_{2+k} \\ &= 2^{2^{2+k}} + 1 \\ &= 2^{2^2 \times 2^k} + 1 \\ &= 16^{2^k} + 1 \\ &= (6+10)^{2^k} + 1 \end{aligned}$$

hence, the congruence with the fixed modulus 10:

$$f_n \equiv 6^{2^k} + 1 \mod 10$$
or simply:
$$f_n \equiv 7 \mod 10 \text{ for n>1}$$

So, for the function $f_n = 2^{2^n}+1$ with n>1, we found only one congruence with a fixed modulus covering all Fermat numbers but $F_0 = 3$ and $F_1 = 5$, so that the set $\{f_n \equiv 7 \mod 10\}$ is a covering system of modulus $\mu = 10$ of all Fermat numbers > 5. According to Dirichlet theorem, this covering system contains infinitely many primes but all these primes are not Fermat primes.

4.4 The appropriate test for Fermat numbers

As Fermat little theorem misses a true reciprocal, this little theorem cannot be used to characterize Fermat prime numbers and we have to find and use a true theorem to do that.

In 1877, The French mathematician Pépin (1826-1904) proved [8] [9] a theorem dedicated to Fermat numbers, today called Pépin's test:
Theorem. Let's consider $k \geqslant 2$ and $F_n = 2^{2^n}+1$ with $n \geqslant 2$. Then, the two following propositions are equivalent:

$$\text{(i) } k^{(F_n-1)/2} \equiv -1 \mod F_n,$$
$$\text{(ii) } F_n \text{ is prime } \textit{and} \left(\frac{k}{F_n}\right) = -1$$

where $\left(\frac{k}{F_n}\right)$ is Legendre' symbol.

To have Pépin's test become explicit, k must be explicitly chosen among several values (3,5,10) to have:

$$\left(\frac{k}{F_n}\right) = -1$$

We have shown that $f_{n+1} \equiv 2 \mod f_{k=0,n}$, therefore we have $F_n \equiv 2 \mod 3$ when $n > 1$. Choosing k=3 and using Gauss' law of reciprocity, we have then:

$$\left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right)(-1)^{\frac{3-1}{2}\times\frac{F_n-1}{2}} = \left(\frac{F_n}{3}\right) = \left(\frac{2}{3}\right) = -1$$

And we can now proceed with the proof.

4.5 Proof of Fermat primes conjecture

Proof. We have found in section 4.3 the congruence:

$$f_n \equiv 7 \mod 10 \text{ for n>1}$$

but this congruence makes no distinction between Fermat primes up to $f_4 = 65537$ and the others. To make this distinction, as n=2 gives $f_2 = 17$, for $n \geqslant 2$, we have:

$$\begin{gathered}
\text{from: } F_n = 2^{2^n} + 1 \\
F_n - 17 = 2^{2^n} - 16 \\
F_n - 17 = 16(2^{2^{n-2}} - 1) \\
F_n - 17 = 16(2^{2^{(n-3)+1}} - 1) \\
F_n - 17 = 16(2^{2\times 2^{(n-3)}} - 1) \\
F_n - 17 = 16((F_{n-3} - 1)^2 - 1)
\end{gathered}$$

and as for any $n \geqslant 2$ we have the congruence $f_n \equiv 7 \mod 10$, we also have:

$$(F_n - 1)^2 - 1 \equiv 0 \mod 5$$

and, for $n - 3 \geqslant 2$ or $n \geqslant 5$:

$$\begin{gathered}
F_n - 17 = 16 \times 5\left(\frac{(F_{n-3} - 1)^2 - 1}{5}\right) \\
F_n = 17 + 80m
\end{gathered}$$

Then, as:

$$3^{(F_n-1)/2} = 3^{(16+80m)/2} = 3^{8+40m} = 3^8(3^{40})^m$$

Pépin's test can be rewritten as follows:
Let's consider $F_n = 2^{2^n}+1$ with $n \geqslant 5$. So:

$$\text{(i) If } 3^8(3^{40})^m \equiv -1 \mod F_n$$
$$\text{then (ii) } F_n \text{ is prime } \textit{and } \left(\frac{3}{F_n}\right) = -1$$
$$\text{and reciprocally.}$$

Then, noticing that the explicit numbers of left member of (i) will not change modulo F_n if $F_n > 3^{40}$ and that:

$$F_5 = 4294967297$$
$$3^{40} = 12157665459056928801$$
$$F_6 = 18446744073709551617$$
$$\text{we have:}$$
$$F_5 < 3^{40} < F_6,$$
$$\text{and:}$$
$$F_n = 17{+}80\text{m} > 3^{40} \quad \text{implies that:} \quad F_n > F_5$$

Hypothesis. If Pépin's test is verified for any prime $F_n > F_5$, we should have:

$$\text{(i) } 3^{(F_n-1)/2} \equiv -1 \mod F_n$$
$$\text{and, as } F_n = 17{+}80\text{m:}$$
$$\text{(i) } 3^{8+40m} \equiv -1 \mod F_n$$

But we have on one hand:

$$\begin{array}{ccc} 3^4 = 81 & \equiv & 1 \mod 80 \\ 3^{8+40m} & = & 3^{4(2+10m)} \\ & = & (3^4)^{2+10m} \\ 3^{8+40m} & \equiv & 1 \mod 80 \\ 3^{8+40m} \mod F_n & \equiv & 1 \mod 80 \mod F_n \end{array}$$

$$\text{and, on the other hand:}$$

$$\begin{array}{ccc} F_n & = & 17{+}80\text{m} \\ F_n - 1 & \equiv & 16 \mod 80 \\ -1 \mod F_n & \equiv & 16 \mod 80 \mod F_n \end{array}$$

and, as we always have:

$$1 \mod 80 \mod F_n \neq 16 \mod 80 \mod F_n.$$

(i) is never verified for any $F_n > F_5$.

This proves that Fermat prime numbers are not infinitely many. □

5 Mersenne prime numbers conjecture

Mersenne prime numbers M_n are the prime numbers generated by the function:

$$f_n = 2^n - 1$$

The Mersenne conjecture is that Mersenne primes are infinitely many.

5.1 A first relation between Mersenne numbers

There is an obvious recurrence relation between Mersenne numbers:

$$f_{n+1} = 2^{n+1} - 1 = 2(2^n - 1) + 1$$
$$f_{n+1} = 2f_n + 1$$

which means that all f_n values are odd and relatively prime with their immediate previous value.

5.2 A second relation between Mersenne numbers

From this relation, we can find the following general relation:

$$\begin{aligned}
f_{n+1} &= 2f_{n+1-1} + 1 \\
&= 2(2f_{n+1-2} + 1) + 1 = 2^2 f_{n+1-2} + 2 + 1 \\
&= 2(2(2f_{n+1-3} + 1) + 1) + 1 = 2^3 f_{n-3} + 4 + 2 + 1 \\
&= 2(2(2(2f_{n+1-4} + 1) + 1) + 1) + 1 = 2^4 f_{n+1-4} + 8 + 4 + 2 + 1 \\
&\cdots \\
&= 2(2(2(2f_{n+1-k} + 1) + 1) + 1) + 1 = 2^k f_{n+1-k} + (2^k - 1)
\end{aligned}$$

or, for any $0 < k < n$, $f_{n-k} < f_n$, $f_k < f_n$ and replacing n+1 by n:

$$f_n = 2^k f_{n-k} + f_k$$

which proves that all f_n values are relatively prime with *all* their previous values f_{n-k}. Making n tend to infinity, this proves that *all* f_n values are relatively prime.

5.3 Composite Mersenne numbers

As when n is even (n=2k), we have from the last relation:

$$f_{2k} = 2^k f_k + f_k$$
$$f_{2k} = f_k(2^k + 1)$$
$$f_{2k} = f_k(f_k + 2)$$

this proves that f_{2k} is always composite.

A more general result is also available:

f_n is prime if and only if n is prime.

Proof. If n is an odd composite (n=ab), we have:

$$\begin{aligned} f_n = f_{ab} &= 2^{ab} - 1 \\ &= (2^a - 1)(1 + 2^a + 2^{2a} + 2^{3a} + ... + 2^{(b-1)a}) \\ &= (2^b - 1)(1 + 2^b + 2^{2b} + 2^{3b} + ... + 2^{(a-1)b}) \end{aligned}$$

so that f_{ab} is always composite and f_n is prime if and only if n is prime. □

5.4 A glimpse of Mersenne numbers

As we have seen that f_n is prime if and only if n is prime, let's build the following table for only prime n's up to 61.

Table 5. Factorizations of $f_n=2^n$-1 for prime n=2,61

Function f	Value	Factorization
f=2^2-1 =	3	prime
f=2^3-1 =	7	prime
f=2^5-1 =	31	prime
f=2^7-1 =	127	prime
f=2^{11}-1 =	2047	= 23×89
f=2^{13}-1 =	8191	prime
f=2^{17}-1 =	131071	prime
f=2^{19}-1 =	524287	prime
f=2^{23}-1 =	8388607	= 47×178481
f=2^{29}-1 =	536870911	= 233×1103×2089
f=2^{31}-1 =	2147483647	prime
f=2^{37}-1 =		= 223×616318177
f=2^{41}-1 =		= 13367×164511353
f=2^{43}-1 =		= 431×9719×2099863
f=2^{47}-1 =		= 2351×4513×13264529
f=2^{53}-1 =		= 6361×69431×20394401
f=2^{59}-1 =		= 179951×3203431780337
f=2^{61}-1 =		prime

This proves that even when n is prime, f_n is not automatically prime. As of 2014, only 44 consecutive Mersenne prime numbers are known among the 2,007,537 prime numbers p up to 32,582,657 which gives the 44th Mersenne prime.

5.5 The appropriate test for Mersenne numbers

As Fermat numbers $F_m = 2^{2^m}+1$ are a similar case of Mersenne numbers $M_n = 2^n - 1$ where $n = 2^m$ and $+1$ becomes -1, the idea to build a test for Mersenne numbers is that this test must be based on Pépin's test of section 4.4.

Adapting Pépin's test to Mersenne numbers, we get in a first step:

With $f_n = 2^n - 1 > 1$, it is supposed that for any prime factor q of
$$f_n - 1 = 2^n - 2 = 2(2^{n-1} - 1) = 2f_{n-1},$$

there exists an integer k = k(q) > 1 such that:
if (i) $k^{2f_{n-1}/q} \equiv -1 \mod M_n$
then (ii) f_n is prime *and* $\left(\frac{k}{M_n}\right) = -1$
and reciprocally.

where $\left(\frac{k}{M_n}\right)$ is Legendre' symbol.

But here, relation (i) implies that we must only consider q=2 because when q is an odd prime, we have, according to the definition of quadratic residues and Euler's congruence for Legendre's symbol:

$$\left(\frac{k^{2f_{n-1}/q}}{M_n}\right) = \left(\frac{(k^{f_{n-1}/q})^2}{M_n}\right) = 1 \equiv k^{2f_{n-1}/q} \mod M_n$$

so that relation (i) is then never verified for any k and any odd prime q.

With q=2, relation (i) becomes:

$$\text{(i) } k^{f_{n-1}} \equiv -1 \mod M_n$$

and as for $n > 2$, the number M_n never divides 3, we choose k=3. So, with q=2 and k=3, relation (i) becomes:

$$\text{(i) } 3^{f_{n-1}} \equiv -1 \mod M_n$$

and the test for Mersenne numbers $> f_2 = 3$ is:

With $n > 2$ and $M_n = 2^n - 1 > 3$,
(i) If $3^{f_{n-1}} \equiv -1 \mod M_n$
then (ii) $f_n = M_n$ is prime *and* $\left(\frac{3}{M_n}\right) = -1$
and reciprocally.

where $\left(\frac{3}{M_n}\right)$ is Legendre' symbol. In a second step, we have to prove that this test is valid.

Proof. For (i): Using Legendre's symbol and the definition of quadratic residues, we have:

$$\left(\frac{3^{f_{n-1}}}{M_n}\right) = \left(\frac{3(3^{f_{n-1}-1})}{M_n}\right) = \left(\frac{3(3^{2^{n-1}-2})}{M_n}\right) = \left(\frac{3(3^{2^{n-2}-1})^2}{M_n}\right) = \left(\frac{3}{M_n}\right)$$

and, as (ii) is verified and with Euler's congruence for Legendre's symbol:

$$\left(\frac{3^{f_{n-1}}}{M_n}\right) = -1 \equiv 3^{f_{n-1}} \mod M_n$$

which proves (i).

For (ii): From the law of reciprocity, we have:

$$\left(\frac{3}{M_n}\right) = \left(\frac{M_n}{3}\right)(-1)^{\frac{3-1}{2}\times\frac{f_n-1}{2}} = \left(\frac{M_n}{3}\right)(-1)^{f_{n-1}} = -\left(\frac{M_n}{3}\right)$$

For $M_n = M_p = 2^p - 1$ where p and M_p are odd primes, we have:

$$M_n \equiv 2^p - 1 \equiv (-1)^p - 1 \equiv -2 \equiv 1^2 \mod 3$$

or:

$$\left(\frac{M_n}{3}\right) = 1$$

and, as looked for:

$$\left(\frac{3}{M_n}\right) = -\left(\frac{M_n}{3}\right) = -1$$

which proves (ii). □

To visualize the results of this test, we can build the following table.

Table 7: Partial visualization of the test for Mersenne numbers

n	Test	Results
n=3	$3^{f_2} \equiv ? -1 \mod f_3$	$3^3 \equiv -1 \mod 7$: $f_3 = prime$
n=5	$3^{f_4} \equiv ? -1 \mod f_5$	$3^{15} \equiv -1 \mod 31$: $f_5 = prime$
n=7	$3^{f_6} \equiv ? -1 \mod f_7$	$3^{63} \equiv -1 \mod 127$: $f_7 = prime$
n=11	$3^{f_{10}} \equiv ? -1 \mod f_{11}$	$3^{1023} \equiv 1565 \mod 2047$
n=13	$3^{f_{12}} \equiv ? -1 \mod f_{13}$	$3^{4095} \equiv -1 \mod 8191$: $f_{13} = prime$
n=17	$3^{f_{16}} \equiv ? -1 \mod f_{17}$	$3^{65535} \equiv -1 \mod 131071$: $f_{17} = prime$
n=19	$3^{f_{18}} \equiv ? -1 \mod f_{19}$	$3^{262143} \equiv -1 \mod 524287$: $f_{19} = prime$

5.6 A congruence with fixed modulus

To get this congruence, we consider the difference between any couple of values f_p and f_n with $n > p$:

$$f_n - f_p = (2^n - 1) - (2^p - 1) = 2^n - 2^p = 2^p(2^{n-p} - 1)$$

from which we have the congruence:

$$f_n \equiv f_p \equiv 2^p - 1 \mod 2^p$$

If we choose $p = 5$, we have for $n > 5$:

$$f_n \equiv 31 \mod 32$$

5.7 Proof of Mersenne conjecture

Here, the Mersenne conjecture refered to is that there are infinitely many Mersenne primes.

Proof. As we have just proved that for $n > 5$ we have the congruence:

$$f_n \equiv 31 \mod 32$$
$$\text{or:}$$
$$f_n = 31 + 32k$$

the relation (i) of the test for Mersenne *prime* numbers can then be written:

$$\text{(i) If } 3^{15+16k} \equiv -1 \mod M_n$$
$$\text{or: (i) If } 3^{15}(3^{16})^k \equiv -1 \mod M_n$$

Then, noticing that the explicit numbers of left member will not change modulo M_n if $M_n > 3^{16}$ and that:

$$M_{25} = 33,554,431 < 3^{16} = 43,046,721 < M_{26} = 67,108,863$$
$$\text{we have:}$$
$$M_n > 3^{16} \quad \text{implies that:} \quad M_n > M_{25}$$

Hypothesis. If Mersenne primes were not infinitely many, there would exist a limit L beyond which there would be no more of them. But we will prove that no such limit L exists.

The only known limit at this time is $L = 3^{16} = 3^{2^{p-1}}$ which comes from the congruence $f_n \equiv 2^p - 1 \mod 2^p$ with the arbitrarily chosen $p = 5$ and which was determined from the maximum explicit number appearing in:

$$\text{(i) If } 3^{15}(3^{16})^k \equiv -1 \mod M_n$$

With this limit, we would then be able to make the hypothesis that for $M_n > M_{25}$, no more Mersenne primes could exist and follow that track.

But we have to remember that in the congruence $f_n \equiv 2^p - 1 \mod 2^p$ with $p < n$, instead of choosing $p = 5$, we can choose any $p < n$ for any positive integer n. This means that when n tends to infinity, p can also be chosen

as tending to infinity, which makes the limit $3^{2^{p-1}}$ also tend to infinity and therefore, that there is no limit, up to infinity, that allows to define a domain where Mersenne primes could not exist.

This proves that the function $f_n = 2^n - 1$ generates infinitely many Mersenne prime numbers. □

5.8 Double Mersenne primes problem

Double Mersenne primes are the prime numbers defined by:

$$M_{M_p} = 2^{M_p} - 1 \text{ where p is a prime}$$

These numbers are generated by the function:

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

The first four double Mersenne primes are:

$$\begin{aligned} M_{M_2} = f_2 = M_3 &= 7 \\ M_{M_3} = f_3 = M_7 &= 127 \\ M_{M_5} = f_5 = M_{31} &= 2147483647 \\ M_{M_7} = f_7 = M_{127} &= 170141183460469231731687303715884105727 \end{aligned}$$

As the first values of p for which M_p is prime are p = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127 and as for p = 13, 17, 19 and 31, double Mersenne numbers are known to be composite, the next candidate double Mersenne number to be prime is $M_{M_{61}} = 2^{2305843009213693951} - 1$. It is so huge that, as of 2015, an unresolved problem is: are double Mersenne primes infinitely many?

Proof. As double Mersenne primes are Mersenne primes and as these last ones are infinitely many as proved in section 5.7, the solution of this problem is that double Mersenne primes are also infinitely many. □

ACKNOWLEDGEMENTS. This work is dedicated to my family. As I am a hobbyist in mathematics, I wish to express my gratitude towards the Editors of this journal as well as towards the team of Reviewers for having welcomed, reviewed and accepted my article.

References

[1] Weisstein, Eric W. *Landau's Problems*, From MathWorld–A Wolfram Web Resource. http://mathworld.wolfram.com/LandausProblems.html

[2] Bouniakowsky V., Sur les diviseurs numériques invariables des fonctions rationnelles entières, *Mémoires de l'Académie Impériale des Sciences de Saint-Pétersbourg, Sixième série, Sciences Mathématiques, Physiques et Naturelles, Tome VIII, Première partie*, **Tome VI**, (1857), 305 - 329.

[3] Riesel, Hans, Några stora primtal, *Elementa*, **39**, (1956), 258-260.

[4] Sierpiński, W.,Sur un problème concernant les nombres k2^n+1, *Elemente der Mathematik*, **15**, (1960), 73-74.

[5] Deloin R., Riesel and Sierpiński problems are solved, *Theoretical Mathematics & Applications*, **5**(3), (2015), 37-50.

[6] Brillhart J. & Selfridge J.L., Some factorizations of $2^m \pm 1$ and related results, *Math. Comp.*, **21**, (1967), 87-96 and 751.

[7] Fermat Pierre de, Lettre à Frenicle, (1640) visited on internet (in French and English) on May 10, 2015 at: https://web.archive.org/web/20061222105104, and http://www.cs.utexas.edu/users/wzhao/fermat2.pdf.

[8] Pépin P., Sur la formule $2^{2^n} + 1$, *Comptes Rendus Acad. Sci. Paris*, **85**, (1877), 329-333.

[9] Wikipedia, *Pépin's test*, visited on July 18, 2015 at: http://en.wikipedia.org/wiki/Pépin's_test