Applied Mathematics & Information Sciences **4**(3) (2010), 307–313
– An International Journal
©2010 Dixie W Publishing Corporation, U. S. A.

On Generalized Fermat Numbers $3^{2^n} + 1$

Amin Witno
Department of Basic Sciences and Mathematics,Philadelphia University, Jordan 19392
Email Address: awitno@gmail.com

Received November 16, 2008; Revised March 28, 2009

The Fermat numbers $F(n) = 2^{2^n} + 1$ have been studied to great extents as far as primality and factorization are concerned. The generalized Fermat numbers are those of the form $F_a(n) = a^{2^n} + 1$, which raise similar interests when a is an even number. If a is odd, of course, $F_a(n)$ would be divisible by 2. In this paper, we investigate the behaviour of the numbers $E_n = F_3(n)/2$ and present an initial primality test for E_n given that E_{n-1} is known to be prime. Some ideas of research for future consideration are suggested.

Keywords: Generalized Fermat numbers, primality testing.

1 Background

Factorization and primality testing have become two major areas of research in the field of computational number theory. Modern primality tests and factorization methods have their roots back in the times of Fermat but it was not until the late seventies—particularly with the invention of the RSA cryptosystem—that the subjects have again gained a wide attention in the world of computing mathematics.

Two families of integers that serve well to illustrate the theories, as well as to pose an endless factoring challenge, are the Fermat numbers $F(n) = 2^{2^n} + 1$ and the Mersenne numbers $M(p) = 2^p - 1$. Fermat conjectured that the sequence $F(n)$ would yield only primes; The defying fact now is that no one has seen a prime Fermat number beyond $F(4)$, if there is any (in contrast to the seemingly infinite list of their counterpart: the Mersenne primes).

Even when its compositeness has been verified, a Fermat number is generally too enormous in size to give away one of its proper factors. For that, an advanced factoring tool such as the elliptic curve method can be utilized, with a great deal of patience, in order to

This paper was presented at the ICRTMS 2008 in Bahrain, an international conference for which the author received financial support through the Deanship of Scientific Research, Philadelphia University, Jordan.

tame large integers as these. Such scenario was properly applied to $F(10)$ in [2], to name one successful case.

The generalized Fermat numbers $F_a(n) = a^{2^n} + 1$ share most of the arithmetic properties enjoyed by $F(n)$. While primality concern for Fermat numbers is considered settled, at least theoretically, that for generalized Fermat numbers on the other hand is quite lacking. Compensating this setback, however, many efforts have been fruitful in finding factors of generalized Fermat numbers. Dubner and Keller [4] discovered that each prime of the form $k \times 2^m + 1$ with $m > n$ is a factor of some $F_a(n)$ for approximately one in every k values of the base a, independent of n. In fact, quite a few generalized Fermat numbers in this way have been revealed to be divisible by existing known prime factors of $F(n)$.

This knowledge furthermore plays a crucial role in the search for primes among the generalized Fermat numbers by way of simultaneously sieving certain intevals of a, for a fixed value of n. Yves Gallot, one of the prominent researchers in this field, has written his *Proth.exe* program for anyone wishing to participate in the hunt for a record prime; see `http://pagesperso-orange.fr/yves.gallot/primes/`.

As an added remark, readers should be aware that some authors employ the name generalized Fermat numbers refering to the larger class of integers $a^{2^n} + b^{2^n}$, where a and b are required to have no common factors. See, for instance, the works cited in [1] and [6].

2 Preliminary Facts

Let $a \geq 2$. If k has an odd prime factor q, then the number $a^k + 1$ will be divisible by $a^{k/q} + 1$. This leads to the definition of *generalized Fermat numbers*

$$F_a(n) = a^{2^n} + 1, \tag{2.1}$$

which extends that of *Fermat numbers* $F(n) = F_2(n) = 2^{2^n} + 1$. The exponent k being a power of 2 allows the possibility of $F_a(n)$ to be a prime number, at least when a is even. The sequence $F_a(n)$ is known to satisfy the following recurrence relation for $n \geq 1$.

$$F_a(n) = (a-1)F_a(0)F_a(1)F_a(2)\cdots F_a(n-1) + 2. \tag{2.2}$$

This recursive definition of $F_a(n)$, furthermore, implies the fact that

$$\gcd(F_a(m), F_a(n)) = \begin{cases} 1, & \text{if } a \text{ is even} \\ 2, & \text{if } a \text{ is odd} \end{cases}, \tag{2.3}$$

whenever $m \neq n$. In particular, note that when a is odd, the terms $F_a(n)$, being all even, are never divisible by 4, except perhaps $F_a(0) = a + 1$.

Results related to the primality of $F_a(n)$ are given next.

Proposition 2.1. *Every odd prime q which divides $F_a(n)$ must satisfy the congruence $q \equiv 1 \pmod{2^{n+1}}$.*

Proof. We have two congruences: $a^{2^n} \equiv -1 \pmod q$ and $a^{2^{n+1}} \equiv 1 \pmod q$. These say that the order of 2 in the multiplicative group Z_q is 2^{n+1}. This order is a divisor of $\phi(q) = q-1$, which yields the theorem. □

Proposition 2.2. *If a is even, the number $F_a(n)$ is a strong probable prime to the base a, for every $n \geq 1$. Moreover, so is $F_a(n)/2$ when a is odd.*

Proof. Let 2^e be the largest power of 2 dividing a. Then $F_a(n) - 1 = a^{2^n} = 2^{e \cdot 2^n} \times d$ for some odd number d. The strong probable prime test involves the sequence

$$a^d,\ a^{2\times d},\ a^{2^2\times d},\ a^{2^3\times d},\ \dots,\ a^{2^{e\cdot 2^n}\times d} = a^{a^{2^n}} \tag{2.4}$$

modulo $F_a(n)$. Since $a^{2^n} \equiv -1 \pmod{a^{2^n}+1}$, we have in this sequence the term $a^{2^n\times d} \equiv -1 \pmod{a^{2^n}+1}$, thereby the test is passed.

For a odd, Eq. (2.2) gives

$$\frac{F_a(n)}{2} - 1 = \frac{(a-1)F_a(0)F_a(1)F_a(2)\cdots F_a(n-1)}{2}. \tag{2.5}$$

In the right-hand numerator of (2.5), while each factor is even, exactly one of them is divisible by 4, i.e., either $a-1$ or $F_a(0) = a+1$. This implies that Eq. (2.5) represents the quantity $2^{n+1} \times c$ for some odd number c. The test is again passed since, similar as before, we have $a^{2^n\times c} \equiv -1 \pmod{(a^{2^n}+1)/2}$. □

Theorem 2.1 (Pepin's primality test for $F(n)$)**.** *For $n \geq 1$, the Fermat number $F(n) = 2^{2^n}+1$ is prime if and only if the following congruence holds.*

$$3^{\frac{F(n)-1}{2}} \equiv -1 \pmod{F(n)}. \tag{2.6}$$

Necessity for this theorem is given by Euler's criterion, noting that the Legendre symbol $(3|2^{2^n}+1)$ is equal to -1. See, for instance, [7, p. 91] for details of the proof. Sufficiency is a direct consequence of the well-known Proth's test, which is a special case of the following weak form of Lucas' test.

Theorem 2.2 (Lucas)**.** *The odd number N is prime if there exists b such that*

$$b^{N-1} \equiv 1 \pmod N \quad \textit{and} \quad b^{\frac{N-1}{q}} \not\equiv 1 \pmod N \tag{2.7}$$

for each prime q dividing $N-1$.

Proof. Let U_N denote the multiplicative group of units of the modular integers Z_N. The first congruence says that the order of b in U_N is a divisor of $N-1$ but not, says the second, of any proper factor of $N-1$. This can happen only if this order is $N-1$. But this quantity is too large for the size of U_N, except when N is prime for then U_N is all of Z_N minus the congruence class of 0. □

3 Primality of $\frac{3^{2^n}+1}{2}$

Let us focus now upon the sequence $F_3(n)/2$. For convenience, we denote these numbers using a new notation,

$$E_n = \frac{3^{2^n}+1}{2}. \tag{3.1}$$

Note that Eq. (2.2) now simplifies slightly to

$$E_n - 1 = F_3(0)F_3(1)F_3(2)\cdots F_3(n-1). \tag{3.2}$$

In turn, this yields a new quadratic recurrence relation for E_n given by

$$E_n = (E_{n-1}-1)\,2E_{n-1}+1. \tag{3.3}$$

Eq. (3.2) poses the biggest problem is applying Lucas' test for the number E_n, since the exponent $E_n - 1$ factors into many distinct primes, increasing with n. In fact to employ Lucas' test, as stated in Theorem 2.2, it would require factoring all the numbers from $F_3(0)$ to $F_3(n-1)$. This concern can be eased to some degree by another theorem due to Pocklington. (See [7, p. 86] for a proof of this theorem.)

Theorem 3.1 (Pocklington)**.** *Suppose that $N-1 = FR$ with $F > R$. Then N is a prime if for every prime factor q of F there is an integer b such that*

$$b^{N-1} \equiv 1 \pmod N \quad \textit{and} \quad \gcd(b^{\frac{N-1}{q}}-1, N) = 1. \tag{3.4}$$

With $N = E_n$ in Pocklington's theorem, the choice of $F = F_3(n-1)$ would serve well. Still, we would need to know the complete factors of E_{n-1} in order to apply the theorem and test the primality of E_n. If we knew, let's assume, that E_{n-1} were prime then we could try the following theorem, which is not expected to work always but is theoretically interesting nevertheless.

Theorem 3.2. *Suppose that E_{n-1} is prime. If $\gcd(9^{E_{n-1}-1}-1, E_n) = 1$ then E_n is also a prime number. Alternately, E_n is prime if there is an integer b, other than 3, such that*

$$b^{E_n-1} \equiv 1 \pmod{E_n} \quad \textit{and} \quad \gcd(b^{2(E_{n-1}-1)}-1, E_n) = 1. \tag{3.5}$$

Proof. In Theorem 3.1, let $N = E_n$ and $F = F_3(n-1) = 2E_{n-1}$. Proposition 2.2 implies that $3^{E_n-1} \equiv 1 \pmod{E_n}$ and $3^{(E_n-1)/2} \equiv (3|E_n) \pmod{E_n}$. After verifying that $E_n \equiv 2 \pmod 3$ and $E_n \equiv 1 \pmod 4$, we call upon the quadratic reciprocity law to evaluate the Jacobi symbol:

$$(3|E_n) = (E_n|3) = (2|3) = -1. \tag{3.6}$$

Therefore $\gcd(3^{(E_n-1)/2}-1, E_n) = \gcd(-2, E_n) = 1$. In view of Theorem 3.1 we need now check only the other prime factor of $F_3(n-1)$, namely E_{n-1}. With the same base of $b = 3$, Eq. (3.3) gives $3^{(E_n-1)/E_{n-1}} = 3^{2(E_{n-1}-1)}$ and thus the desired $\gcd$ condition, which is sufficient to prove primality. If, however, we choose another base $b \neq 3$ then the condition $b^{E_n-1} \equiv 1 \pmod{E_n}$ is also needed (this is the Fermat test for probable primes) lest E_n is actually composite. □

Remark 3.1. In the context of Theorem 3.2, the quantity $b^{2(E_{n-1}-1)} - 1$ is divisible by E_{n-1} according to Fermat's little theorem (including the case $b = 3$), say with a quotient of K. The numbers E_n being pairwise relatively prime, the stated $\gcd$ condition in (3.5) may well be replaced by $\gcd(K, E_n) = 1$. In terms of computation time, however, this change would be technically insignificant.

To illustrate the applicability of Theorem 3.2 we run a few tests, comparing the results against the actual primality of E_n; these are recorded in Table 3.1 below. It seems interesting that, using $b = 3$, where they are already strong probable primes to this base, the numbers E_n are likely to be immune against this test.

n	Primality of E_n	Tested with $b = 3$	Tested with $b = 2$
0	prime	N/A	N/A
1	prime	$\gcd = 1$, prime	$\gcd = 1$, prime
2	prime	$\gcd = E_2$, inconclusive	$\gcd = 1$, prime
3	composite	$\gcd = E_3$, inconclusive	composite, Fermat test
4	prime	N/A	N/A
5	prime	$\gcd = E_5$, inconclusive	$\gcd = 1$, prime
6	prime	$\gcd = E_6$, inconclusive	$\gcd = 1$, prime
7	composite	$\gcd = E_7$, inconclusive	composite, Fermat test

Table 3.1: Primality of E_n, compared to test results given by Theorem 3.2.

4 Factorization and Research Problems

Despite all we have, the computations around these numbers yet involve a very large modulus and hence, having recognized a composite E_n, it remains a huge challenge to find its factorization. Table 4.1, given next, displays the first few factorizations of E_n, computed using Keith Matthews' *CALC* program for Windows, available at `http://www.numbertheory.org/calc/`.

There remain many unsolved problems about generalized Fermat numbers. For future research, the following are a number of ideas to pursue where E_n is concerned.

1. We have verified that the numbers E_{10} to at least E_{15} are all composite by means of the Fermat test for probable primes base 2. It would be an interesting problem

to know whether or not there exist Fermat pseudoprimes to the base 2 among the numbers E_n. If there is none, then of course the Fermat test would become an absolute primality test for E_n.

2. If the above idea proved fruitless, can we still find another deterministic test for E_n somewhat similar to that of Pepin?
3. In view of the nice recurrence given by Eq. (3.2), it is tempting to find some ways to predict the occurrence of consecutive primes among the sequence E_n. Although, in this case, it seems more reasonable to conjecture that there are no such things as consecutive primes beyond E_6. If this conjecture is true, then E_n will be composite for infinitely many values of n.
4. Perhaps E_n is never again prime for all $n > 6$.
5. Brute factorization efforts are evidently unwise. We might adopt the techniques utilized in [4] in order to scan values of n for which E_n is divisible by a known proper factor.

n	E_n
0	2
1	5
2	41
3	17×193
4	21523361
5	926510094425921
6	1716841910146256242328924544641
7	$257 \times 275201 \times 138424618868737 \times 3913786281514524929 \times$ 153849834853910661121
8	$12289 \times 8972801 \times C_{111}$
9	$134382593 \times 22320686081 \times C_{226}$

Table 4.1: Prime factorization of E_n up to $n = 9$. The notation C_k indicates a composite (hence incomplete factorization) whose decimal size is k digits long.

References

[1] A. Björn and H. Riesel, Factors of generalized Fermat numbers, *Math. Comp.* **67** (1998), 441–446.

[2] R. P. Brent, Factorization of the tenth Fermat number, *Math. Comp.* **68** (1999), 429–451.

[3] H. Dubner and Y. Gallot, Distribution of generalized Fermat prime numbers, *Math. Comp.* **71** (2001), 825–832.

[4] H. Dubner and W. Keller, Factors of generalized Fermat numbers, *Math. Comp.* **64** (1995), 397–405.

[5] H. Riesel, Common prime factors of the numbers $A_n = a^{2^n}+1$, *BIT* **9** (1969), 264–269.

[6] H. Riesel and A. Björn, *Generalized Fermat Numbers*, in: Mathematics of Computation 1943–1993: A Half-Century of Computational Mathematics, W. Gautschi, editor, American Mathematical Society, RI, 1994, 583–587.

[7] A. Witno, *Theory of Numbers*, BookSurge Publishing, Charleston, SC, 2008.

Amin Witno is an Assistant Professor at the Faculty of Science, Philadelphia University, in Jordan. Dr. Witno's areas of research are largely concentrated in Number Theory, with a particular interest in the topic of primality testing. He is the author of *Theory of Numbers,* an undergraduate textbook for an elementary number theory course, published by BookSurge in 2008.