

# Notes on Generalized Fermat Numbers

H. Eleuch

Max Planck Institute for Physics of Complex Systems, 01187 Dresden, Germany

Received: Jan. 13, 2012; Revised April 28, 2012; Accepted 1 March 2012

Published online: 1 Sep. 2012

**Abstract:** In this paper, we show that any positive prime number takes the form of a generalized Fermat number (GFN)  $F_{a,n} = a^{2^n} + 1$  for some  $a$  and we give a family of non prime GFN.

**Keywords:** Prime numbers, Fermat numbers

## 1. Introduction

There are two different definitions of generalized Fermat numbers (GFN), one of which is more general than the other. In [5], Ribenboim defines a generalized Fermat number as a number of the form  $F_{a,n} = a^{2^n} + 1$  with  $a > 2$ , while Riesel ([6]) further generalizes, defining it to be a number of the form  $a^{2^n} + b^{2^n}$ . Both definitions generalize the usual Fermat numbers  $F_n = 2^{2^n} + 1$ . The only known Fermat primes are  $F_0, F_1, F_2, F_3$  and  $F_4$ . Generalized Fermat numbers  $F_{a,n}$  can be prime only for even  $a$ . It is generally expected that there are an infinite number of primes of this form for each  $n$ . In fact, this is a consequence of the famous "Hypothesis H" in 1958 of Sierpiński and Schinzel. In 1962, Bateman and Horn indicated a quantitative form of "Hypothesis H" which could be used to predict the number of primes for given polynomials [1]. Many of the largest known prime numbers are generalized Fermat numbers. The largest known as of January 2009 is  $24518^{2^{18}} + 1$  (<http://primes.utm.edu/primes/page.php?id=84401>), which has 1150678 decimal digits. The following table gives the first few generalized Fermat primes for various even bases  $a$ :

$a$	prime $a^{2^n} + 1$
2	5, 17, 257, 65537, 4294967297, ...
4	17, 257, 65537, 4294967297, 18446744073709551617...
6	37, 1297, 1679617, 2821109907457,

Note that if  $a = \alpha^\beta$ , then  $F_{a,n} = \alpha^{\beta 2^n} + 1$  and it can be shown that if  $\beta$  takes the form  $\beta = (2\gamma + 1)2^k$  for some

$k \in N$  and  $\gamma \in N \setminus \{0\}$ , then

$$\alpha^{(2\gamma+1)2^k} + 1 \equiv 0 \pmod{\alpha^{2^k} + 1}$$

and hence  $\alpha^\beta + 1$  is not prime. Then the primality of  $F_{a,n}$  implies that  $\beta$  takes the form  $\beta = 2^k$  and in this case  $F_{a,n} = a^{2^n} + 1 = \alpha^{2^{n+k}} + 1 = F_{\alpha,n+k}$ . Then we can consider define GFN  $F_{a,n}$  for a particular choice of  $a$ , that is  $a$  is even and not of the  $\alpha^\beta$  where  $\alpha$  and  $\beta$  are positive integers with  $\alpha, \beta \geq 2$ . In this paper we shall focus our study on the properties of GFN of this form.

## 2. Divisibility and properties of GFN

We begin this section by recalling some results

### Lemma 2.1

Let  $n, k \in N^*$ , then the following are equivalent

- i.  $X^n + 1 \equiv 0 \pmod{X^k + 1}$
- ii.  $n \equiv 0 \pmod{k}$  and  $\frac{n}{k}$  is an odd positive integer.

**Proof:** If we set  $n = qk + r$  with  $0 \leq r < k$ , then the result follows from the following rule:

$$X^n + 1 = (X^k + 1) \sum_{j=1}^q (-1)^{j-1} X^{n-jk} + (-1)^q X^r + 1.$$

\* Corresponding author: e-mail: [heleuch@fulbrightmail.org](mailto:heleuch@fulbrightmail.org)

### Corollary 2.2

Let  $n, k \in N^*$  and assume that

i.  $X^n + 1 \equiv 0 \pmod{X^k + 1}$  for some integer  $1 \leq k < n$  then  $n \neq 2^p$  for all  $p \in N^*$

ii. Let  $n \in N^*$ , if for any integer  $k$  with  $2 \leq k < n$ , one has  $X^n + 1 \neq 0 \pmod{X^k + 1}$ , then  $n$  is prime or  $n = 2^p$  for some  $p \in N^*$ .

**Proof:** i. If  $X^n + 1 \equiv 0 \pmod{X^k + 1}$ , then by the preceding Lemma, we have  $n = (2\alpha + 1)k$ , now let  $k = 2^{p_1}k_1$  with  $k_1$  is an odd integer. Then if  $n = 2^p$  for some  $p$ , we must have  $(2\alpha + 1)k_1 = 2^{p-p_1}$  and hence  $p - p_1 = \alpha = 0$  and  $k_1 = 1$ , that is  $n = k$  which is a contradiction.

ii. Suppose that for any integer  $k$  with  $k, 2 \leq k < n$ , one has  $X^n + 1 \neq 0 \pmod{X^k + 1}$  and write  $n = kq + r$  with  $0 \leq r < k$ . Again by the previous Lemma we must have  $r \neq 0$  and hence  $n$  is prime or  $r = 0$  and for any divisor  $k$  of  $n$  one has  $\frac{n}{k}$  is not an odd integer, that is each divisor of  $n$  is even and hence  $n$  takes the form  $n = 2^p$  for some  $p \in N^*$ .

Now we give the following

### Lemma 2.3

Let  $k, n \in N$  with  $k \neq n$  and  $a \in N$ , then

$$\gcd(a^{2^k} + 1, a^{2^n} + 1) = \begin{cases} 1, & \text{if } a \text{ is odd} \\ 2, & \text{if } a \text{ is even} \end{cases}$$

**Proof:** Let  $n, k \in N^*$ , with  $k \leq n$  then we have

$$a^{2^n} + 1 = (a^{2^k} + 1) \sum_{j=1}^{2^{n-k}} (-1)^{j-1} a^{2^n-j2^k} + 2.$$

Thus, it follows that

$$\begin{aligned} \gcd(a^{2^n} + 1, a^{2^k} + 1) &= \gcd(a^{2^k} + 1, 2) \\ &= \begin{cases} 1, & \text{if } a \text{ is even} \\ 2, & \text{if } a \text{ is odd} \end{cases} \end{aligned}$$

Consider the set

$$\begin{aligned} E &= \{a \in 2N, a \geq 2, \text{ and } a \neq \alpha^\beta \\ &\quad \text{where } \alpha, \beta \in N, \alpha \geq 2, \beta \geq 2\}. \end{aligned}$$

Then we can show the following

### Proposition 2.4

Any positive odd prime number  $p$  can be written in a unique way of the form  $p = a^n + 1$  where  $a \in E$  and  $n \in N \setminus \{0\}$ .

**Proof:** Set  $x = p - 1$ , and write  $x = 2^{k_1}p_2^{k_2} \dots p_r^{k_r}$  be the decomposition of  $x$  into prime factors. Note that  $k_1 \geq 1$ , since  $x$  is even. Put  $d = \gcd(k_1, \dots, k_r)$ , then one has the following two cases.

### Case 1: $d \geq 2$

Then, we write

$$x = (2^{\frac{k_1}{d}} \prod_{i=2}^r p_i^{\frac{k_i}{d}})^d.$$

It is clear that  $a = 2^{\frac{k_1}{d}} \prod_{i=2}^r p_i^{\frac{k_i}{d}} \in E$  and hence  $p = a^n + 1$  where  $n = d$ .

### Case 2: $d = 1$

In this case, we have  $p = (p-1)^1 + 1$  and  $p-1 \in E$ .

Now let  $p$  be a positive prime number  $p$  and suppose that we can write  $p = a^n + 1 = b^m + 1$ , where  $a, b \in E$  and  $n, m \in N \setminus \{0\}$ . This implies that  $a^n = b^m$  and hence  $a = b^{\frac{m}{n}} \in E$  or  $b = a^{\frac{n}{m}} \in E$  which show that  $n = m$  and  $a = b$ .

### Remark 2.1

Any positive integer  $N > 2$  can be written in a unique way of the form

$$N = a^m + 1,$$

where  $m$  is a natural number and  $a$  is not of the form  $\alpha^\beta$  with  $\alpha, \beta \geq 2$ .

Now we see from Proposition 2.4, that if  $p$  is a positive odd prime number then  $p$  is of the form  $p = a^m + 1$  where  $a \in E$ . On the other hand if  $m = 2^n(2\gamma + 1)$  for some positive integer  $\gamma$  then  $a^m + 1 \equiv 0 \pmod{a^{2^n} + 1}$ , and hence  $a^m + 1$  is not prime. Thus if we let  $m = 2^n$ , then the family  $\{a^{2^n} + 1\}_{a \in E, n \in N}$  may contains prime numbers and together with proposition 2.4 we have the following:

### Corollary 2.5

If  $p > 2$  is a prime number then  $p$  is a generalized Fermat number  $F_{a,n}$  where  $a \in E$ . From now on we shall focus our study on this family of numbers  $\{a^{2^n} + 1\}$  with  $a \in E$ .

### Lemma 2.6

If  $a^{2^n} + 1 \equiv 0 \pmod{q}$  then for any  $k \in N$ , one has

$$a^{2^{n+k}} + 1 \equiv 2 \pmod{q}.$$

**Proof:** Let  $F_{a,n} = a^{2^n} + 1$ , then one can show that

$$F_{a,n} - 2 = (a-1)F_{a,1} \dots F_{a,n-1}.$$

Now if  $F_{a,n} \equiv 0 \pmod{q}$ , then for any  $k \in N$

$$F_{a,n+k} \equiv 2 \pmod{q}.$$

### Lemma 2.7

Let  $a \in E$  and assume that for some integer  $\alpha$  one has  $a^{2^n} + 1 \equiv 0 \pmod{\alpha}$ , then for any integer number  $k$  one has  $(a + 2k\alpha)^{2^n} + 1 \equiv 0 \pmod{\alpha}$ .

**Proof:** For any integer number  $k$ , one has  $a + 2k\alpha \equiv a \pmod{\alpha}$  and hence  $(a + 2k\alpha)^{2^n} + 1 \equiv a^{2^n} + 1 \pmod{\alpha}$ , then if  $a^{2^n} + 1 \equiv 0 \pmod{\alpha}$  it follows that

$$(a + 2k\alpha)^{2^n} + 1 \equiv 0 \pmod{\alpha}.$$

For example, since  $F_5$  has the prime factor 641, then

$$2^{32}(1 + 641k)^{32} + 1 \equiv 0 \pmod{641},$$

and hence  $\{F_{2+1282k, 5}\}_{k \in N}$  are not prime numbers. Similarly we can generate a series of non prime numbers arising from the non prime known Fermat numbers  $F_6, F_7, \dots$

### Corollary 2.8

Suppose that there exist some even positive integer  $\beta$ , a positive integer  $s$  which is not of the form  $s = 2^r$  ( $r \neq 0$ ) and  $k \in N \setminus \{0\}$  such that

$$\beta^s \pm 2k(\beta^{2^n} + 1) = a \in E$$

then  $a^{2^n} + 1$  is not prime.

Moreover  $\beta^{2^n} + 1$  divides  $a^{2^n} + 1$ .

Here we give examples of non prime GFN. For instance if  $s = 2^n + 1$  we obtain

$$(\beta^{2^n}(\beta - 2k) - 2k)^{2^n} + 1 \equiv 0 \pmod{\beta^{2^n} + 1},$$

$$n \in N, k \in Z \setminus \{0\}.$$

For instance, take  $\beta = 6$  and  $k = 2$ , then  $6^{2^n} + 1 \mid 2^{2^n}(2 \times 6^{2^n} - 4)^{2^n} + 1$  for all  $n$ . Similarly we can see that

$$(4 \times 10^{2^n} - 6)^{2^n} + 1 \equiv 0 \pmod{10^{2^n} + 1},$$

and so on...

### 3. Conclusion

In this paper, we have shown that we can refine our research for prime numbers within generalized Fermat numbers  $F_{a,n} = a^{2^n} + 1$  for a class of even positive integers  $a$  which are not of the form  $\alpha^\beta$  where  $a, \beta \geq 2$ .

Finally our belief that the following conjecture is true

### Conjecture

If  $F_{a,n}$  is not prime for some  $n$  then  $F_{a,k}$  is not prime for any  $k$  with  $k \geq n$ .

### Acknowledgment

The author is grateful to Dr Béchir Dali for useful discussions.

### References

- [1] D. BROADHURST, "GFN Conjecture." Post to primeform user forum. Apr. 1, 2006.
- [2] P. T. BATEMAN AND R. A. HORN, A Heuristic Asymptotic Formula Concerning the Distribution of Prime Numbers, Math. Comp. 16 (1962), pp. 363–367. MR 26:6139.
- [3] D. HARVEY AND Y. GALLOT, Distribution of Generalized Fermat numbers, Math. Comp. Vol. 71, No. 238, pp.825–832 (2001).
- [4] D. HARVEY AND W. KELLER, Factors of Generalized Fermat numbers, Math. Comp. Vol. 64, No. 209, pp.397–408 (1995).
- [5] P. RIBENBOIM, The New Book of Prime Number Records. New York: Springer-Verlag, 1996.
- [6] H. RIESEL, Prime Numbers and Computer Methods for Factorization, 2nd ed. Boston, MA: Birkhäuser (1994).
- [7] A. WITNO, On Generalized fermat numbers  $3^{2^n} + 1$ . Applied Math. & Information sciences, Vol. 4, No. 3, pp. 307–313 (2010).