Michal Křížek; Jan Chleboun

A note on factorization of the Fermat numbers and their factors of the form $3h2^n + 1$

Mathematica Bohemica, Vol. 119 (1994), No. 4, 437–445

Persistent URL: `http://dml.cz/dmlcz/126115`

A NOTE ON FACTORIZATION OF THE FERMAT NUMBERS AND THEIR FACTORS OF THE FORM $3h2^n + 1$

MICHAL KŘÍŽEK, JAN CHLEBOUN, Praha

(Received May 9, 1994)

Summary. We show that any factorization of any composite Fermat number $F_m = 2^{2^m} + 1$ into two nontrivial factors can be expressed in the form $F_m = (k2^n + 1)(\ell 2^n + 1)$ for some odd k and ℓ, $k \geqslant 3$, $\ell \geqslant 3$, and integer $n \geqslant m+2$, $3n < 2^m$. We prove that the greatest common divisor of k and ℓ is 1, $k + \ell \equiv 0 \bmod 2^n$, $\max(k, \ell) \geqslant F_{m-2}$, and either $3 \mid k$ or $3 \mid \ell$, i.e., $3h2^{m+2} + 1 \mid F_m$ for an integer $h \geqslant 1$. Factorizations of F_m into more than two factors are investigated as well. In particular, we prove that if $F_m = (k2^n + 1)^2(\ell 2^j + 1)$ then $j = n + 1$, $3 \nmid \ell$ and $5 \nmid \ell$.

Keywords: Fermat numbers, prime numbers, factorization, squarefreeness

AMS classification: 11A51, 11Y05

Throughout the paper all variables $i, j, k, n, n_1, \ldots$ are supposed to be positive integers except for m and z which can moreover attain the value zero. For $m = 0, 1, 2, \ldots$, the mth Fermat number is defined by $F_m = 2^{2^m} + 1$. The aim of this paper is to derive some properties of factors of composite Fermat numbers.

Recall that $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$ are primes and other primes F_m (if they exist) are not known yet. For instance, in 1732 Euler found that $F_5 = 641 \cdot 6700417$, where the both factors are prime. The Fermat number F_6 was factored by Landry in 1880 (see e.g. [10]), F_7 by Morrison and Brillhart in 1970 [8], F_8 by Brent and Pollard in 1980 [2], F_9 by Lenstra, Lenstra, Jr., Manasse, Pollard in 1990 [7] and F_{11} by Brent in 1988 [1]. The complete factorizations of F_m are known only for the above mentioned numbers for the time being. Their structure, however, remainds a deterministic chaos. Some prime factors of F_{10} and of more than 100 other Fermat numbers can be found in excellent surveys [3, 6]. From all of the above-mentioned papers we have

$$(1) \quad 1 = \Omega_0 = \ldots = \Omega_4 < 2 = \Omega_5 = \ldots = \Omega_8 < 3 = \Omega_9 < 5 = \Omega_{11} < 6 < \Omega_{12},$$

where Ω_m is the number of prime divisors of F_m (counted with multiplicity). Anyhow, the monotonocity of the whole sequence $\{\Omega_m\}$ is an open problem as well as the squarefreeness of F_m.

In 1877, Lucas established a general form of prime divisors of the Fermat numbers, namely that: Every prime divisor p of F_m, $m > 1$, satisfies the congruence (see e.g. [4, p. 376])

$$p \equiv 1 \bmod 2^{m+2}. \tag{2}$$

The main idea of its proof is the following. As in [7, p. 320] we put $b = 2^{2^{m-2}}\left(2^{2^{m-1}} - 1\right)$. Then $b^2 = 2^{2^{m-1}}\left(2^{2^m} - 2 \cdot 2^{2^{m-1}} + 1\right)$ and we get

$$b^2 \equiv 2 \bmod p, \tag{3}$$

since $2^{2^m} + 1 \equiv 0 \bmod p$. From here we have $b^{2^{m+1}} \equiv 2^{2^m} \equiv -1 \bmod p$ which implies that

$$b^{2^{m+2}} \equiv 1 \bmod p. \tag{4}$$

According to (3), the numbers b and p are coprime and thus by the little Fermat theorem (i.e., $b^{p-1} \equiv 1 \bmod p$) and (4) it is possible to deduce that $2^{m+2} \mid p - 1$. Therefore, (2) holds.

We start with several simple lemmas.

Lemma 1. *If $2^n + 1$ divides F_m for some $n \geqslant 1$ and $m \geqslant 0$ then $F_m = 2^n + 1$.*

Proof. Set $Q_n = 2^n + 1$, i.e., $F_m = Q_{2^m}$. From the binomial theorem we obtain

$$Q_{ij} = 2^{ij} + 1 = (Q_j - 1)^i + 1 \equiv 1 + (-1)^i \bmod Q_j$$

and thus

$$\gcd(Q_{ij}, Q_j) = \begin{cases} 1 & \text{for } i \text{ even}, \\ Q_j & \text{for } i \text{ odd}. \end{cases} \tag{5}$$

Hence,

$$\gcd(F_z, F_m) = 1 \quad \text{for } z \neq m, \tag{6}$$

i.e., no two different Fermat numbers have a common divisor greater than 1 (see also [5, p. 14]).

Suppose that $Q_n \mid F_m$ for some $n < 2^m$. Then $n = i2^z$, where i is odd and $z < m$. Using (5) for $j = 2^z$, we see that $Q_{2^z} \mid Q_n$. However, this contradicts (6), since $Q_{2^z} = F_z$ and $Q_n \mid F_m$. Therefore, $n = 2^m$. □

Lemma 2. *Let F_m be composite. Then there exist natural numbers j, k, ℓ, n such that*

$$F_m = (k2^n + 1)(\ell 2^j + 1), \quad k \geqslant 3,\ \ell \geqslant 3,\ k \text{ and } \ell \text{ are odd.} \tag{7}$$

Proof. Since F_m is odd and composite, it can be written as a product of two odd numbers $k2^n + 1$ and $\ell 2^j + 1$ for some natural numbers n, j and odd integers k, ℓ. However, according to Lemma 1 the case $k = 1$ or $\ell = 1$ is not possible. Hence, $k \geqslant 3$ and $\ell \geqslant 3$. □

Definition 3. Let $q > 1$ be an odd integer. A uniquely determined exponent n from the decomposition $q = k2^n + 1$, where k is odd, is called the order of q.

In the next lemma we prove that the orders of two odd factors are not greater than the order of their product.

Lemma 4. *Let*

$$k2^n + 1 = (k_1 2^{n_1} + 1)(k_2 2^{n_2} + 1), \tag{8}$$

where k, k_1, k_2 are odd. Then $n \geqslant \min(n_1, n_2)$, where the sharp inequality holds if and only if $n_1 = n_2$. Moreover, $k > k_1 k_2 2^{\max(n_1, n_2)}$ whenever $n_1 \neq n_2$.

Proof. Without loss of generality assume that $n_1 \geqslant n_2$. Then

$$k2^n + 1 = (k_1 k_2 2^{n_1} + k_1 2^{n_1 - n_2} + k_2)2^{n_2} + 1. \tag{9}$$

Since k is odd, $n \geqslant n_2 = \min(n_1, n_2)$. The number in the brackets from (9) is even if and only if $n_1 = n_2$. If $n_1 > n_2$ then $n = n_2$ and thus $k > k_1 k_2 2^{n_1}$ by (9). □

Theorem 5. *Let F_m be composite and let $k2^n + 1$ be its arbitrary factor (not necessarily prime) where k is odd. Then $k \geqslant 3$, n is an integer for which*

$$m + 2 \leqslant n < \tfrac{1}{3} 2^m \tag{10}$$

and there exists an odd $\ell \geqslant 3$, such that

$$F_m = (k2^n + 1)(\ell 2^n + 1), \tag{11}$$

i.e., the both factors have the same order. Moreover,

$$k + \ell \equiv 0 \bmod 2^n, \tag{12}$$

k and ℓ are coprime, i.e.,

$$\gcd(k,\ell) = 1, \tag{13}$$

$$\max(k,\ell) \geqslant F_{m-2} \tag{14}$$

and

$$\text{either} \quad 3 \mid k \quad \text{or} \quad 3 \mid \ell, \tag{15}$$

i.e., for any composite Fermat number F_m there exists a natural number h such that $3h2^n + 1 \mid F_m$.

Proof. Let $\ell 2^j + 1$ be a cofactor to $k2^n + 1$ such that ℓ is odd. According to (7), we have

$$F_m = k\ell 2^{n+j} + k2^n + \ell 2^j + 1.$$

Without loss of generality we may assume that $n \geqslant j$. Then

$$2^{2^m - j} = k\ell 2^n + k2^{n-j} + \ell,$$

where the terms 2^{2^m-j} and $k\ell 2^n$ are even because $2^m > j$ and $n \geqslant 1$. This implies that $n = j$, since ℓ is odd. (The role of k and ℓ is thus the same.)

From the relation

$$2^{2^m - n} = k\ell 2^n + k + \ell,$$

we deduce that $2^m - n > n$ which implies (12). Moreover, if $q \mid k$ and $q \mid \ell$ for some odd q then $q \mid 2^{2^m-n}$. Hence, $q = 1$ and we observe that (13) holds.

Further we establish the proposed bounds (10) for n. By (12), $k + \ell \geqslant 2^n$. Since $k \neq \ell$ due to (13), we have

$$\max(k,\ell) > 2^{n-1}, \tag{16}$$

and thus

$$F_m = (k2^n + 1)(\ell 2^n + 1) > (2^{n-1}2^n + 1)(2 \cdot 2^n + 1) > 2^{3n} + 1.$$

Consequently, $3n < 2^m$.

By (2) each prime factor of F_m is of the form $r2^{m+2} + 1$ for some integer r. Hence, if $k2^n + 1$ is a prime factor then $m + 2 \leqslant n$, since k is odd. Suppose that $k2^n + 1$ is a product of two primes which is of the form (8). Then Lemma 4 implies $m + 2 \leqslant \min(n_1, n_2) \leqslant n$. By induction we find that $m + 2 \leqslant n$ for any factor of F_m, i.e., (10) is valid.

If $n \leqslant 2^{m-2}$ then by (11), (13) and (10)

$$\max(k,\ell) > 2^{-n}(\sqrt{F_m}-1) > 2^{-2^{m-2}}(2^{2^{m-1}}-1) = 2^{2^{m-2}} - 2^{-2^{m-2}}$$

and thus $\max(k,\ell) \geqslant F_{m-2}$, since $\max(k,\ell) \geqslant 2^{2^{m-2}}$ and k and ℓ are odd. Conversely, if $n \geqslant 2^{m-2}+1$ then by (16),

$$\max(k,\ell) > 2^{n-1} \geqslant 2^{2^{m-2}},$$

i.e., (14) holds.

Finally we prove (15). Obviously,

$$3 \mid 2^n + (-1)^{n+1}. \tag{17}$$

Hence, $3 \mid F_m - 2$ (taking $n = 2^m$) and thus $(k2^n+1)(\ell 2^n+1) \equiv 2 \bmod 3$. This and (17) imply

$$(1+(-1)^n k)(1+(-1)^n \ell) \equiv 2 \bmod 3. \tag{18}$$

We easily find that $xy \equiv 2 \bmod 3$ if and only if $x \equiv 2 \bmod 3$ and $y \equiv 1 \bmod 3$ or $x \equiv 1 \bmod 3$ and $y \equiv 2 \bmod 3$. From here and (18) we observe that just one of the numbers k and ℓ is divisible by 3. □

Corollary 6. *Let the assumptions of Theorem 5 be satisfied and let $3 \mid \ell$. Then*

$$k = 3u+1 \quad \text{for some } u \text{ even} \iff n \text{ is even}, \tag{19}$$

$$k = 3u+2 \quad \text{for some } u \text{ odd} \iff n \text{ is odd}. \tag{20}$$

Proof. As $3 \mid \ell$, we have from (15) that $k = 3u + y$, $1 \leqslant y \leqslant 2$ and from (18)

$$1 + (-1)^n k \equiv 2 \bmod 3.$$

This yields (19) and (20). □

Remark 7. Although the upper bound on n in (10) is too rough, we observe that no n satisfies (10) if $m \leqslant 4$ (which implies that $F_0, \ldots, F_4$ are primes without carrying out any trial divisions). For the prime factor $641 = 5 \cdot 2^7 + 1$ of F_5 we have the equality $n = m + 2$. On the other hand, the sharp inequality $n > m + 2$ holds e.g. for the factorization of F_8 into two primes with $n = 11$. By (11) and (10)

$$\min(k,\ell) < (2^n \min(k,\ell)+1)/2^n < \sqrt{F_m}/2^n < F_{m-1}/2^{m+2}.$$

Moreover, $\min(k,\ell) \geqslant 3$, where the equality is achieved e.g. for prime factors of F_{38} and F_{207} (see [3, p. lxxxviii]). According to (11) and (13), no Fermat number is a square of a natural number.

Theorem 8. *Let $n_1 \leqslant n_2 \leqslant n_3$ and let*

$$F_m = \prod_{j=1}^{3} (k_j 2^{n_j} + 1), \tag{21}$$

where k_j are odd. Then $k_j \geqslant 3$ for $j = 1, 2, 3$,

$$m + 2 \leqslant n_1 = n_2 < n_3, \tag{22}$$

and either no k_j is divisible by 3 or just two k_j are divisible by 3.

Moreover, if $k_1 = k_2$ (i.e., if F_m is not squarefree) then $n_3 = n_1 + 1$, $3 \nmid k_3$ and $5 \nmid k_3$.

Proof. Obviously $k_j \geqslant 3$ and $n_j \geqslant m + 2$ by Theorem 5. Let us rewrite (21) as a product of two factors

$$F_m = (k_1 2^{n_1} + 1)[(k_2 k_3 2^{n_3} + k_2 + k_3 2^{n_3 - n_2}) 2^{n_2} + 1]. \tag{23}$$

The number $k_2 k_3 2^{n_3} + k_2 + k_3 2^{n_3 - n_2}$ cannot be even, since then $n_3 = n_2$ and by Theorem 5 we would get $n_1 \geqslant n_2 + 1$ which contradicts the assumption $n_1 \leqslant n_2$. Therefore, $k_2 k_3 2^{n_3} + k_2 + k_3 2^{n_3 - n_2}$ is an odd number and thus $k_3 2^{n_3 - n_2}$ is even. This implies that $n_3 > n_2$. By Theorem 5 and (23) we have $n_1 = n_2$.

From (23) and (15) we see that all three k_j cannot be divisible by 3. Suppose now that just one k_j is divisible by 3. Let for instance $3 \nmid k_1$, $3 \mid k_2$ and $3 \nmid k_3$. Then $k_2 k_3 2^{n_3} + k_2 + k_3 2^{n_3 - n_2}$ is not divisible by 3 which contradicts (15) and (23). In a similar way we get a contradiction for the cases $3 \nmid k_1$, $3 \nmid k_2$, $3 \mid k_3$, and $3 \mid k_1$, $3 \nmid k_2$, $3 \nmid k_3$.

Finally, suppose that $k_1 = k_2$ in (21). Then obviously $3 \nmid k_3$ and from (11) and the relation

$$F_m = [k_1 (k_1 2^{n_1 - 1} + 1) 2^{n_1 + 1} + 1](k_3 2^{n_3} + 1)$$

we find that $n_3 = n_1 + 1$.

Recall that the last digit of $k_1 2^{n_1} + 1$ belongs to the set $\{1, 3, 7, 9\}$, since $5 \nmid F_m$ for $m \neq 1$ by (6). Hence,

$$(k_1 2^{n_1} + 1)^2 \bmod 10 \in \{1, 9\}.$$

From here, (21) and the trivial fact that $F_m \equiv 7 \bmod 10$ for $m > 1$, we have $k_3 2^{n_3} + 1 \bmod 10 \in \{3, 7\}$ which yields $5 \nmid k_3$. ◻

R e m a r k 9. The Fermat number F_9 is a product of three prime factors $k_j 2^{n_j}+1$, $j = 1,2,3$, cf. (1). According to [7, p. 321], their orders are $n_1 = n_2 = 11 = m+2$ and $n_3 = 16$ and thus by (11), we get

$$(24)\quad F_9 = (k_1 2^{11}+1)(\ell_1 2^{11}+1) = (k_2 2^{11}+1)(\ell_2 2^{11}+1) = (k_3 2^{16}+1)(\ell_3 2^{16}+1)$$

for some $\ell_j \geqslant 3$ odd. Hence, any factor $\ell 2^n + 1$ of F_m for which $n = m+2$ need not be a prime factor yet. We also see that for given $n \geqslant m+2$ the Diophantine equation (11) with unknowns k and ℓ can have no or one or more solutions. It is also interesting that no k_j from (24) is divisible by 3. This can be directly verified from the explicit expressions of the prime factors of F_9 (see [7]) and thus $3 \mid \ell_j$ for $j = 1,2,3$ by (15). According to (22), no Fermat number is a cube of a natural number.

Theorem 10. *Let $n_1 \leqslant n_2 \leqslant \ldots \leqslant n_N$, $N > 1$ and let*

$$(25)\qquad F_m = \prod_{j=1}^{N} (k_j 2^{n_j} + 1),$$

where k_j are odd. Then $m+2 \leqslant n_j$, $k_j \geqslant 3$ for $j = 1,\ldots,N$, and the number of factors $k_j 2^{n_j}+1$, whose order is n_1, is even. No two factors from (25) form a twin prime pair.

P r o o f. We again have by Theorem 5 that $m+2 \leqslant n_j$ and $k_j \geqslant 3$ for all $j = 1,\ldots,N$. For $N < 4$ the proof of the first part of Theorem 10 follows from Theorems 5 and 8. So let $N \geqslant 4$. Suppose, on the contrary, that $2z+1$ (for an integer $z \geqslant 0$) is the number of factors of the lowest order n_1, i.e., $n_{2z+1} < n_{2z+2}$ if $2z+1 < N$. Then by Lemma 4 we have for $z \geqslant 1$ that

$$\operatorname{ord}((k_{2i}2^{n_1}+1)(k_{2i+1}2^{n_1}+1)) > n_1 \quad \text{for any } i = 1,\ldots,z,$$

where analogously to [7, p. 321] the operator ord denotes the order from Definition 3, i.e., $\operatorname{ord}(k2^n+1) = n$ for k odd. Using Lemma 4 again, we find by induction that

$$\operatorname{ord}\Big(\prod_{j=2}^{2z+1} (k_j 2^{n_1}+1)\Big) > n_1$$

and thus also

$$(26)\qquad \operatorname{ord}\Big(\prod_{j=2}^{N} (k_j 2^{n_j}+1)\Big) > n_1$$

for $z \geqslant 1$. However, we easily find that (26) holds even if $z \geqslant 0$. This contradicts (25) and (11), as $\text{ord}(k_1 2^{n_1} + 1) = n_1$.

Let $n_j \leqslant n_i$. Then

$$|(k_i 2^{n_i} + 1) - (k_j 2^{n_j} + 1)| = |(k_i 2^{n_i - n_j} - k_j) 2^{n_j}| \geqslant 2^{n_j} \geqslant 2^{m+2}$$

whenever $n_i \neq n_j$ or $k_i \neq k_j$. From here we see that the product (25) cannot contain a twin prime pair. □

Remark 11. The 21-digit factor of F_{11} (see [1]) is of order 14. The other four factors have order 13.

Two prime factors of F_{10} are already known and their orders are 12 and 14 (see [3]). The associated cofactor is known to be composite, i.e., $\Omega_{10} = N \geqslant 4$, cf. (1) and (25). Note that the first prime factor of F_{10} is of the form $k_1 2^{n_1} + 1 = 11131 \cdot 2^{12} + 1$. By Theorem 10 there exists its another prime factor of order $m + 2 = 12$, $k_2 2^{12} + 1$, $k_2 \geqslant 3$ odd, where k_2 is for the time being unknown. However, by (20) and (11), k_2 cannot be of the form $k_2 = 3v + 2$, since $n_2 = 12$ is even.

From Theorem 10 we observe that there exist at least four factors of F_{12} of order $m + 2 = 14$, as three of them are already known [3].

Finally note that k_j in (25) need not be coprime (cf. (13)). For instance we have $3 \mid k_j$ for two factors of F_{11} and $7 \mid k_j$ for other its two factors, and $7 \mid k_j$ for three of the known factors of F_{12}, etc.

Acknowledgement. This research was supported by grant No. 201/94/1067 of the Grant Agency of the Czech Republic. The authors thank the referee for valuable suggestions and the reference [9].

References

[1] *R. P. Brent*: Factorization of the eleventh Fermat number. Abstracts Amer. Math. Soc. *10* (1989), 176–177.

[2] *R. P. Brent, J. M. Pollard*: Factorization of the eight Fermat number. Math. Comp. *36* (1981), 627–630.

[3] *J. Brillhart, D. H. Lehmer, J. L. Selfridge, B. Tuckerman, S. S. Wagstaff*: Factorization of $b^n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 11, 12$ up to high powers. Contemporary Math. vol. 22, Amer. Math. Soc., Providence, 1988.

[4] *L. E. Dickson*: History of the theory of numbers, vol. I, Divisibility and primality. Carnegie Inst., Washington, 1919.

[5] *G. H. Hardy, E. M. Wright*: An introduction to the theory of numbers. Clarendon Press, Oxford, 1945.

[6] *W. Keller*: Factors of Fermat numbers and large primes of the form $k.2^n + 1$. II. Preprint Univ. of Hamburg, 1992, 1–40.

[7] *A. K. Lenstra, H. W. Lenstra, Jr., M. S. Manasse, J. M. Pollard*: The factorization of the ninth Fermat number. Math. Comp. *61* (1993), 319–349.

[8] *M. A. Morrison, J. Brillhart*: A method of factoring and the factorization of F_7. Math. Comp. *29* (1975), 183–205.
[9] *N. Robbins*: Beginning number theory. W. C. Brown Publishers, 1993.
[10] *H. C. Williams*: How was F_6 factored? Math. Comp. *61* (1993), 463–474.

Authors' address: *Michal Křížek*, *Jan Chleboun*, Mathematical Institute, Academy of Sciences of the Czech Republic, Žitná 25, CZ-115 67 Prague 1, Czech Republic, e-mail: `krizek@earn.cvut.cz`, `chleboun@earn.cvut.cz`.