Scientia Magna
Vol. 4 (2008), No. 2, 25-28

On the Smarandache function and the Fermat number

Jinrui Wang

Department of Mathematics, Northwest University, Xi'an, Shaanxi, P.R.China

Abstract For any positive integer n, the famous F.Smarandache function $S(n)$ is defined as the smallest positive integer m such that $n \mid m!$. That is, $S(n) = \min\{m : n \mid m!, n \in N\}$. The main purpose of this paper is using the elementary method to study the estimate problem of $S(F_n)$, and give a sharper lower bound estimate for it, where $F_n = 2^{2^n} + 1$ is called the Fermat number.

Keywords F. Smarandache function, the Fermat number, lower bound estimate, elementary method.

§1. Introduction and result

For any positive integer n, the famous F.Smarandache function $S(n)$ is defined as the smallest positive integer m such that $n \mid m!$. That is, $S(n) = \min\{m : n \mid m!, n \in N\}$. For example, the first few values of $S(n)$ are $S(1) = 1$, $S(2) = 2$, $S(3) = 3$, $S(4) = 4$, $S(5) = 5$, $S(6) = 3$, $S(7) = 7$, $S(8) = 4$, $S(9) = 6$, $S(10) = 5$, $S(11) = 11$, $S(12) = 4$, $\cdots$. About the elementary properties of $S(n)$, many authors had studied it, and obtained some interesting results, see references [1], [2], [3], [4] and [5]. For example, Lu Yaming [2] studied the solutions of an equation involving the F.Smarandache function $S(n)$, and proved that for any positive integer $k \geq 2$, the equation

$$S(m_1 + m_2 + \cdots + m_k) = S(m_1) + S(m_2) + \cdots + S(m_k)$$

has infinite group positive integer solutions $(m_1, m_2, \cdots, m_k)$.

Dr. Xu Zhefeng [3] studied the value distribution problem of $S(n)$, and proved the following conclusion:

Let $P(n)$ denotes the largest prime factor of n, then for any real number $x > 1$, we have the asymptotic formula

$$\sum_{n \leq x} (S(n) - P(n))^2 = \frac{2\zeta\left(\frac{3}{2}\right) x^{\frac{3}{2}}}{3 \ln x} + O\left(\frac{x^{\frac{3}{2}}}{\ln^2 x}\right),$$

where $\zeta(s)$ denotes the Riemann zeta-function.

Chen Guohui [4] studied the solvability of the equation

$$S^2(x) - 5S(x) + p = x, \tag{1}$$

and proved the following conclusion:

Let p be a fixed prime. If $p = 2$, then the equation (1) has no positive integer solution; If $p = 3$, then the equation (1) has only one positive integer solution $x = 9$; If $p = 5$, then the equation (1) has only two positive integer solutions $x = 1,\ 5$; If $p = 7$, then the equation (1) has only two positive integer solutions $x = 21,\ 483$. If $p \geq 11$, then the equation (1) has only one positive integer solution $x = p(p-4)$.

Le Maohua [5] studied the lower bound of $S(2^{p-1}(2^p-1))$, and proved that for any odd prime p, we have the estimate:

$$S\left(2^{p-1}(2^p-1)\right) \geq 2p+1.$$

Recently, in a still unpublished paper, Su Juanli improved the above lower bound as $6p+1$. That is, she proved that for any prime $p \geq 7$, we have the estimate

$$S\left(2^{p-1}(2^p-1)\right) \geq 6p+1.$$

The main purpose of this paper is using the elementary method to study the estimate problem of $S(F_n)$, and give a sharper lower bound estimate for it, where $F_n = 2^{2^n}+1$ is the Fermat number. That is, we shall prove the following:

Theorem. For any positive integer $n \geq 3$, we have the estimate

$$S(F_n) \geq 8 \cdot 2^n + 1,$$

where $F_n = 2^{2^n}+1$ is called the Fermat number.

§2. Proof of the theorem

In this section, we shall complete the proof of our theorem directly. First note that the Fermat number $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$, they are all prime. So for $n = 3$ and 4, we have $S(F_3) = 257 \geq 8 \cdot 2^3 + 1$, $S(F_4) = 65537 > 8 \cdot 2^4 + 1$. Now without loss of generality we can assume that $n \geq 5$. If F_n be a prime, then from the properties of $S(n)$ we have $S(F_n) = F_n = 2^{2^n}+1 \geq 8 \cdot 2^n + 1$. If F_n be a composite number, then let p be any prime divisor of F_n, it is clear that $(2,\ p) = 1$. Let m denotes the exponent of 2 modulo p. That is, m denotes the smallest positive integer r such that

$$2^r \equiv 1 \pmod{p}.$$

Since $p \mid F_n$, so we have $F_n = 2^{2^n}+1 \equiv 0 \pmod{p}$ or $2^{2^n} \equiv -1 \pmod{p}$, and $2^{2^{n+1}} \equiv 1 \pmod{p}$. From this and the properties of exponent (see Theorem 10.1 of reference [6]) we have $m \mid 2^{n+1}$, so m is a divisor of 2^{n+1}. Let $m = 2^d$, where $1 \leq d \leq n+1$. It is clear that $p \dagger 2^d - 1$, if $d \leq n$. So $m = 2^{n+1}$ and $m \mid \phi(p) = p-1$. Therefore, $2^{n+1} \mid p-1$ or

$$p = h \cdot 2^{n+1} + 1. \tag{2}$$

Now we discuss the problem in following three cases:

(A) If F_n has more than or equal to three distinct prime divisors, then note that $2^{n+1}+1$ and $2\cdot 2^{n+1}+1$ can not be both primes, since one of them can be divided by 3. So from (2) we know that in all prime divisors of F_n, there exists at least one prime divisor p_i such that $p_i = h_i\cdot 2^{n+1}+1 \geq 4\cdot 2^{n+1}+1 = 8\cdot 2^n+1$.

(B) If F_n has just two distinct prime divisors, without loss of generality we can assume

$$F_n = \left(2^{n+1}+1\right)^{\alpha}\cdot\left(3\cdot 2^{n+1}+1\right)^{\beta} \quad \text{or} \quad F_n = \left(2\cdot 2^{n+1}+1\right)^{\alpha}\cdot\left(3\cdot 2^{n+1}+1\right)^{\beta}.$$

If $F_n = \left(2^{n+1}+1\right)^{\alpha}\cdot\left(3\cdot 2^{n+1}+1\right)^{\beta}$, and $\alpha\geq 4$ or $\beta\geq 2$, then from the properties of $S(n)$ we have the estimate

$$\begin{aligned} S(F_n) &\geq \max\left\{S\left(\left(2^{n+1}+1\right)^{\alpha}\right),\ S\left(\left(3\cdot 2^{n+1}+1\right)^{\beta}\right)\right\} \\ &= \max\left\{\alpha\cdot\left(2^{n+1}+1\right),\ \beta\cdot\left(3\cdot 2^{n+1}+1\right)\right\} \\ &\geq 8\cdot 2^n+1. \end{aligned}$$

If $F_n = 2^{2^n}+1 = \left(2^{n+1}+1\right)\cdot\left(3\cdot 2^{n+1}+1\right) = 3\cdot 2^{2n+2}+2^{n+3}+1$, then note that $n\geq 5$, we have the congruence

$$0 \equiv 2^{2^n}+1-1 = 3\cdot 2^{2n+2}+2^{n+3} \equiv 2^{n+3} \pmod{2^{n+4}}.$$

This is impossible.

If $F_n = 2^{2^n}+1 = \left(2^{n+1}+1\right)^2\cdot\left(3\cdot 2^{n+1}+1\right) = 3\cdot 2^{3n+3}+3\cdot 2^{2n+3}+3\cdot 2^{n+1}+2^{2n+2}+2^{n+2}+1$, then we also have

$$0 \equiv 2^{2^n}+1-1 = 3\cdot 2^{3n+3}+3\cdot 2^{2n+3}+3\cdot 2^{n+1}+2^{2n+2}+2^{n+2} \equiv 3\cdot 2^{n+1} \pmod{2^{n+2}}.$$

This is still impossible.

If $F_n = 2^{2^n}+1 = \left(2^{n+1}+1\right)^3\cdot\left(3\cdot 2^{n+1}+1\right)$, then we have

$$2^{2^n}+1 \equiv \left(3\cdot 2^{n+1}+1\right)^2 \equiv 3\cdot 2^{n+2}+1 \pmod{2^{n+4}}$$

or

$$0 \equiv 2^{2^n} \equiv \left(3\cdot 2^{n+1}+1\right)^2-1 \equiv 3\cdot 2^{n+2} \pmod{2^{n+4}}.$$

Contradiction with $2^{n+4} \dagger 3\cdot 2^{n+2}$.

If $F_n = \left(2\cdot 2^{n+1}+1\right)^{\alpha}\cdot\left(3\cdot 2^{n+1}+1\right)^{\beta}$, and $\alpha\geq 2$ or $\beta\geq 2$, then from the properties of $S(n)$ we have the estimate

$$\begin{aligned} S(F_n) &\geq \max\left\{S\left(\left(2\cdot 2^{n+1}+1\right)^{\alpha}\right),\ S\left(\left(3\cdot 2^{n+1}+1\right)^{\beta}\right)\right\} \\ &= \max\left\{\alpha\cdot\left(2\cdot 2^{n+1}+1\right),\ \beta\cdot\left(3\cdot 2^{n+1}+1\right)\right\} \\ &\geq 8\cdot 2^n+1. \end{aligned}$$

If $F_n = 2^{2^n}+1 = \left(2\cdot 2^{n+1}+1\right)\cdot\left(3\cdot 2^{n+1}+1\right)$, then we have

$$F_n = 2^{2^n}+1 = 3\cdot 2^{2n+3}+5\cdot 2^{n+1}+1.$$

From this we may immediately deduce the congruence

$$0 \equiv 2^{2^n} = 3\cdot 2^{2n+3}+5\cdot 2^{n+1} \equiv 5\cdot 2^{n+1} \pmod{2^{2n+3}}.$$

This is not possible.

(C) If F_n has just one prime divisor, we can assume that

$$F_n = \left(2^{n+1}+1\right)^{\alpha} \quad \text{or} \quad F_n = \left(2\cdot 2^{n+1}+1\right)^{\alpha} \quad \text{or} \quad F_n = \left(3\cdot 2^{n+1}+1\right)^{\alpha}.$$

If $F_n = \left(2^{n+1}+1\right)^{\alpha}$, then it is clear that our theorem holds if $\alpha \geq 4$. If $\alpha = 1$, 2 or 3, then from the properties of the congruence we can deduce that $F_n = \left(2^{n+1}+1\right)^{\alpha}$ is not possible.

If $F_n = \left(2\cdot 2^{n+1}+1\right)^{\alpha}$ or $\left(3\cdot 2^{n+1}+1\right)^{\alpha}$, then our theorem holds if $\alpha \geq 2$. If $\alpha = 1$, then F_n be a prime, so our theorem also holds.

This completes the proof of Theorem.

References

[1] F. Smarandache, Only Problems, Not Solutions, Chicago, Xiquan Publishing House, 1993.

[2] Lu Yaming, On the solutions of an equation involving the Smarandache function. Scientia Magna, **2**(2006), No.1, 76-79.

[3] Xu Zhefeng, The value distribution property of the Smarandache function, Acta Mathematica Sinica, Chinese Series, **49**(2006), No.5, 1009-1012.

[4] Chen Guohui and Liu Baoli, An equation involving the F.Smarandache function and its positive integer solutions, Scientia Magna, **4** (2008), No.1, 76-78.

[5] Le Mohua, A lower bound for $S\left(2^{p-1}(2^p-1)\right)$, Smarandache Notions Journal, **12**(2001), No.1-2-3, 217-218.

[6] T. M. Apostol, Introduction to Analytic Number Theory, New York, Springer-Verlag, 1976.

[7] Zhang Wenpeng, The elementary number theory (in Chinese), Shaanxi Normal University Press, Xi'an, 2007.

[8] I. Balacenoiu and V. Seleacu, History of the Smarandache function, Smarandache Notions Journal, **10**(1999), No.1-2-3,192-201.