第 24卷第 2期　　四川理工学院学报(自然科学版)　　Vol. 24　No. 2
2011年 4月　　Journal of Sichuan University of Science & Engineering (Natural Science Edition)　　Apr. 2011
文章编号: 1673-1549(2011)02-0140-02

费马数与伪素数

管训贵

(泰州师范高等专科学校, 江苏　泰州　225300)

摘　要: 如果合数 N 满足 $2^N \equiv 2(\mathrm{mod}\ N)$, 则称 N 为伪素数. 本文运用数论中的一些简单结果, 如任何费马合数都是伪素数以及费马小定理(若 p 为素数, a 为整数, 且 $(a, p) = 1$, 则 $a^{p-1} \equiv 1(\mathrm{mod}\ p)$)等, 给出了 $N = F_{S_1}F_{S_2}\cdots F_{S_k}$ 为伪素数的充要条件: $S_1 \leqslant 2^{S_2} - 1$ 且 $S_k \leqslant 2^{S_1} - 1$, 这里 $S_1 < S_2 < \cdots < S_k$, $F_{S_i} = 2^{2^{S_i}} + 1$ 为费马数。

关键词: 费马数; 伪素数; 合数; 充要条件

中图分类号: O151　　文献标识码: A

引　言

目前我们仅知道 $n = 0, 1, 2, 3, 4$ 时, 费马数 $F_n = 2^{2^n} + 1$ 是素数, 而 n 为其它正整数时, 所发现的费马数均为合数。文[1]证明了任何费马合数都是伪素数, 并推出了 $F_mF_n(m \neq n)$ 是伪素数的充要条件, 本文给出多个费马数之积为伪素数的充要条件。

定理　设 $S_1 < S_2 < \cdots < S_k$, 这里 $S_i(i = 1, \cdots, k)$ 均为正整数, 则 $N = F_{S_1}F_{S_2}\cdots F_{S_k}$ 为伪素数的充要 $S_1 \leqslant 2^{S_2} - 1$ 且 $S_k \leqslant 2^{S_1} - 1$。

1　定义与引理

定义 1[1]　设 N 为正整数, 我们把满足 $2^N \equiv 2(\mathrm{mod}\ N)$ 的合数 N 称为伪素数。

定义 2[2]　设 p 为素数, a 为整数, 且 $(a, p) = 1$, 若 d 是使 $a^d \equiv 1(\mathrm{mod}\ p)$ 成立的最小正整数, 则称 d 是 a 关于模 p 的阶。

引理 1[1]　任何费马合数都是伪素数。

引理 2[2]　设 m, n 是非负整数, n 当 $m \neq n$ 时, $(F_m, F_n) = 1$。

引理 3[3]　(费马小定理)设 p 为素数, a 为整数, 若 $(a, p) = 1$, 则 $a^{p-1} \equiv 1(\mathrm{mod}\ p)$。

引理 4[4]　设 n 是非负整数, 则 2 关于模 F_n 的阶为 2^{n+1}。

引理 5[5]　若 $a^k \equiv 1(\mathrm{mod}\ m)$, 而 a 关于模 m 的阶为 d, 则 $d \mid k$。

2　定理的证明

若 $S_1 < S_2 < \cdots < S_k$, 则由引理 1与引理 2知, F_{S_1}, F_{S_2}, …, F_{S_k} 是互素的奇素数或奇伪素数。由引理 4知, 2 关于模 $F_{S_i}(i = 1, \cdots, k)$ 的阶为 2^{S_i+1}。

(必要性)

如果 $N = F_{S_1}F_{S_2}\cdots F_{S_k}$ 为伪素数, 即 $2^N \equiv 2(\mathrm{mod}\ N)$, 则有

$$2^N \equiv 2(\mathrm{mod}\ F_{S_i}),\quad i = 1, \cdots k \tag{1}$$

根据引理 3, 得

$$2^{F_{S_i}-1} \equiv 2(\mathrm{mod}\ F_{S_i}),\quad i = 1, \cdots k$$

故(1)变为

$$\begin{aligned}2 &\equiv 2^{\frac{N}{F_{S_i}}\cdot F_{S_i}} \equiv (2^{F_{S_i}-1})^{\frac{N}{F_{S_i}}}\cdot 2^{\frac{N}{F_{S_i}}}\\ &\equiv 2^{\frac{N}{F_{S_i}}}(\mathrm{mod}\ F_{S_i})\end{aligned}$$

即

$$2^{\frac{N}{F_{S_i}}-1} \equiv 1(\mathrm{mod}\ F_{S_i}),\quad i = 1, \cdots k \tag{2}$$

又 2关于模 $F_{S_i}(i = 1, \cdots, k)$ 的阶为 2^{S_i+1}, 故由引理 5得

$$2^{S_i+1} \,\Big|\, \left(\frac{N}{F_{S_i}} - 1\right),\quad i = 1, \cdots k。$$

因为 $\dfrac{N}{F_{S_1}} - 1 = \prod\limits_{j=2}^{k} F_{S_j} - 1$

$$= \prod_{j=2}^{k}(2^{2^{S_j}} + 1) - 1 = 2^{2^{S_2}}\cdot Q$$

收稿日期: 2010-12-20

作者简介: 管训贵(1963-), 男, 江苏兴化人, 副教授, 主要从事基础数论方面的研究。

这里 Q 为某一正奇数, 所以 $2^{S_1+1} | 2^{2^{S_2}}\cdot Q$, 即 $2^{S_1+1} | 2^{2^{S_2}}$, 于是

$$S_1 \leqslant 2^{S_2} - 1 \qquad (3)$$

因为 $\frac{N}{F_{S_i}} - 1 = \prod_{j=1, j\neq i}^{k} F_{S_j} - 1$

$$= \prod_{j=1, j\neq i}^{k} (2^{2^{S_j}} + 1) - 1 = 2^{2^{S_1}} \cdot R$$

这里 R 为某一正奇数, $i = 2, \cdots k$, 所以 $2^{S_i+1} | 2^{2^{S_1}}\cdot R$, 即 $2^{S_i+1} | 2^{2^{S_1}}$, 于是 $S_i \leqslant 2^{S_1} - 1$, $i = 2, \cdots k$。

考虑到 $S_1 < S_2 < \cdots < S_k$, 有

$$S_k \leqslant 2^{S_1} - 1 \qquad (4)$$

由(3)、(4)知, 若 $N = F_{S_1}F_{S_2}\cdots F_{S_k}$ 为伪素数, 则 $S_1 \leqslant 2^{S_2} - 1$ 且 $S_k \leqslant 2^{S_1} - 1$。

(充分性)

已知 $S_1 \leqslant 2^{S_2} - 1$ 且 $S_k \leqslant 2^{S_1} - 1$, 结合 $S_1 < S_2 < \cdots < S_k$, 有

$$S_1 \leqslant 2^{S_2} - 1,\ S_2 \leqslant 2^{S_1} - 1,\ \cdots,\ S_k \leqslant 2^{S_1} - 1。$$

即

$$S_1 + 1 \leqslant 2^{S_2},\ S_i + 1 \leqslant 2^{S_1}$$

$$i = 2, \cdots k$$

因为

$$N - 1 = F_{S_1}F_{S_2}\cdots F_{S_k} - 1 = 2^{2^{S_1}} \cdot M$$

这里 M 为某一正奇数, 所以

$$2^{S_i+1} | (N - 1),\ i = 2, \cdots k。$$

考虑到 $S_1 + 1 \leqslant 2^{S_1}$, 有 $2^{S_1+1} | (N - 1)$, 故

$$2^{S_i+1} | (N - 1),\ i = 1, \cdots k。$$

又 2关于模 $F_{S_i}(i = 1, \cdots, k)$ 的阶为 2^{S_i+1}, 即

$$2^{2^{S_i+1}} \equiv 1 (\bmod F_{S_i}),\ i = 1, \cdots k$$

故

$$2^{N-1} \equiv 1 (\bmod F_{S_i}),\ i = 1, \cdots k$$

而 $F_{S_1}, F_{S_2}, \cdots, F_{S_k}$ 两两互素, 因此有

$$2^{N-1} \equiv 1 (\bmod N) \text{ 即}$$

$$2^N \equiv 2 (\bmod N)$$

于是 $N = F_{S_1}F_{S_2}\cdots F_{S_k}$ 为伪素数。

比如, $F_3F_4F_5$, $F_3F_4F_5F_6$, $F_3F_4F_5F_6F_7$ 均为伪素数。

参考文献:

[1] 王云葵. 任何费马数都是素数或伪素数[J]. 玉林师专学报:自然科学版, 1998(3): 26-28.

[2] 柯召, 孙琦. 数论讲义[M]. 北京:高等教育出版社, 1988.

[3] 闵嗣鹤, 严士健. 初等数论[M]. 北京:高等教育出版社, 2004.

[4] 潘承洞, 潘承彪. 初等数论[M]. 北京:北京大学出版社, 1992.

[5] 熊全淹. 初等整数论[M]. 湖北:湖北教育出版社, 1985.

Fermat Number and Pseudoprime Number

GUAN Xun-gui

(Taizhou Normal College, Taizhou 225300, China)

Abstract If a composite number N satisfies $2^N \equiv 2(\bmod N)$, then N is called Pseudoprime number. In this paper, by using the simple result among the number theory, as every Fermat composite number is a Pseudoprime number and Fermat's Little Theorem (If p is prime and a is a positive integer with $(a, p) = 1$, then $a^{p-1} \equiv 1(\bmod p)$ etc, we give a sufficient and necessary condition of the proposition that $N = F_{S_1}F_{S_2}\cdots F_{S_k}$ is a pseudoprime number, it is $S_1 \leqslant 2^{S_2} - 1$ and $S_k \leqslant 2^{S_1} - 1$, where $S_1 < S_2 < \cdots < S_k$ and $F_{S_i} = 2^{2^{S_i}} + 1$ is Fermat number.

Key words Fermat number, Pseudoprime number, composite, sufficient and necessary condition