DOI:10.11721/cqnuj20140310

广义 Fermat 数与伪素数*

刘妙华，焦红英
(空军工程大学 理学院，西安 710051)

摘要:设 m 是正整数,b 是正偶数,$G_m=b^{b^m}+1$。本文运用初等的方法证明了:i)G_m 必为素数或者底为 b 的伪素数;ii)对于适合 $m_1<m_2<\cdots<m_k$ 的正整数 $m_1,m_2,\cdots,m_k$,乘积 $G_{m_1}G_{m_2}\cdots G_{m_k}$ 是底为 b 的伪素数的充要条件是 $m_k\leqslant b^{m_1}-1$。

关键词:广义 Fermat 数;乘积;伪素数
中图分类号:O156.2　　**文献标志码**:A　　**文章编号**:1672-6693(2014)03-0049-03

设 n 是正整数。根据 Euler 定理可知:当 n 是素数时,如果 a 是适合 $gcd(a,n)=1$ 的整数,则必有

$$a^{n-1}\equiv 1(\mathrm{mod}\ n) \tag{1}$$

另外,当 n 是合数时,如果 n 满足同余关系(1),则称 n 是底为 a 的伪素数。长期以来,关于伪素数的各种性质一直是数论中引人关注的研究课题[1]。一些学者也得到了关于伪素数的一些奇妙性质[2-5]。

对于正整数 m,设 $F_m=2^{2^m}+1$ 是第 m 个 Fermat 数。对此,王云葵证明了:任何 Fermat 数必为素数或者底为 2 的伪素数[6]。管训贵证明了:如果 $m_1,m_2,\cdots,m_k$ 是适合 $m_1<m_2<\cdots<m_k$ 的正整数,则 k 个 Fermat 数的乘积 $F_{m_1}F_{m_2}\cdots F_{m_k}$ 是底为 2 的伪素数的充要条件是 $m_1\leqslant 2^{m_2}-1$ 且 $m_k\leqslant 2^{m_1}-1$[7]。这里应该指出:上述结果都是已知的[8],而且因为 $m_1<m_2$,所以文献[3]结果中的条件"$m_1\leqslant 2^{m_2}-1$"是多余的。

对于正整数 b 和 m,其中 $b>1$,设

$$G_m=b^{b^m}+1 \tag{2}$$

由于 Fermat 数 F_m 是 G_m 在 $b=2$ 时的特例,所以形如(2)的 G_m 统称为广义 Fermat 数。对此,本文运用初等方法证明了下列结果。

定理 1　当 b 是偶数时,G_m 必为素数或者底为 b 的伪素数。

定理 2　当 b 是偶数时,如果 $m_1,m_2,\cdots,m_k$ 是适合 $m_1<m_2<\cdots<m_k$ 的正整数,则 k 个广义 Fermat 数的乘积 $G_{m_1}G_{m_2}\cdots G_{m_k}$ 是底为 b 的伪素数的充要条件是 $m_k\leqslant b^{m_1}-1$。

显然,文献[6-8]中的结果分别是本文定理在 $b=2$ 时的特例。

1 定理 1 的证明

设 n 是大于 1 的正整数,a 是适合 $gcd(a,n)=1$ 的整数。根据 Euler 定理可知

$$a^{\varphi(n)}\equiv 1(\mathrm{mod}\ n) \tag{3}$$

其中 $\varphi(n)$是 Euler 函数。因为 $\varphi(m)$必为正整数,所以从(3)式可知存在正整数 r 可使同余关系

$$a^r\equiv 1(\mathrm{mod}\ n) \tag{4}$$

成立。如果 $r=d$ 是可使(4)式成立的最小正整数,则称 d 是整数 a 对模 n 的指数。

引理 1[9]　当 d 是 a 对模 n 的指数时,正整数 r 适合(4)式的充要条件是 $d\mid r$。

引理 2　整数 b 对模 G_m 的指数等于 $2b^m$。

证明　设 d 是 b 对模 G_m 的指数。因为 $b^{2b^m}-1=(b^{b^m}-1)(b^{b^m}+1)=(b^{b^m}-1)G_m$,所以

* **收稿日期**:2013-04-13　**修回日期**:2013-05-06　**网络出版时间**:2014-5-8 14:38
作者简介:刘妙华,女,讲师,研究方向为数论,E-mail:llmmhh_419@163.com
网络出版地址:http://www.cnki.net/kcms/detail/50.1165.N.20140508.1438.011.html

$$b^{2b^m}\equiv 1(\mathrm{mod}\ G_m) \tag{5}$$

根据引理1,从(5)式可知 $d\mid 2b^m$,故有

$$2b^m=ds \tag{6}$$

其中 s 是正整数。

假如 $d\neq 2b^m$,则从(6)式可知 $s\geqslant 2$ 以及 $d\leqslant b^m$。然而,因为根据指数的定义可知 $b^d\equiv 1(\mathrm{mod}\ G_m)$,故从(2)式可得 $G_m=b^{b^m}+1>b^{b^m}-1\geqslant b^d-1\geqslant G_m$ 这一矛盾。由此可知 $d=2b^m$。 证毕

证明 (定理1) 当 b 是偶数时,因为 $b\geqslant 2$,$b^{b^m}\geqslant b^{m+1}$ 且 $b^{m+1}\mid b^{b^m}$,所以

$$2b^m\mid b^{b^m} \tag{7}$$

由于从引理2可知,整数 b 对模 G_m 的指数等于 $2b^m$,所以根据引理1,由(2)、(7)式可得

$$b^{G_m-1}\equiv 1(\mathrm{mod}\ G_m) \tag{8}$$

因此,从(8)式可知 G_m 必为素数或者底为 b 的伪素数。 证毕

2 定理2的证明

引理3[9] 对于正整数 $n_1,n_2,\cdots,n_k$,如果整数 X 和 Y 满足 $X\equiv Y(\mathrm{mod}\ n_i)$,$i=1,2,\cdots,k$,则必有 $X\equiv Y(\mathrm{mod}\ n)$,其中 n 是 $n_1,n_2,\cdots,n_k$ 的最小公倍数。

引理4 当 b 是偶数时,对于不同的正整数 m 和 m',必有 $gcd(G_m,G_{m'})=1$。

证明 因为 $m\neq m'$,所以不妨假定 $m<m'$。设 $l=gcd(G_m,G_{m'})$。由于当 b 是偶数时,l 必为奇数,所以从(2)式可知

$$0\equiv G_{m'}\equiv b^{b^{m'}}+1\equiv(b^{b^m})^{b^{m'-m}}+1\equiv(G_m-1)^{b^{m'-m}}+1\equiv(-1)^{b^{m'-m}}+1\equiv 2(\mathrm{mod}\ l) \tag{9}$$

从(9)式即得 $l=1$。 证毕

引理5 对于适合 $m_1<m_2<\cdots<m_k$ 的正整数 $m_1,m_2,\cdots,m_k$,设

$$n=G_{m_1}G_{m_2}\cdots G_{m_k} \tag{10}$$

当 b 是偶数时,b 对模 n 的指数等于 $2b^{m_k}$。

证明 设 b 对模 n 的指数等于 d,此时,从(10)式可知

$$b^d\equiv 1(\mathrm{mod}\ G_{m_i}),i=1,2,\cdots,k \tag{11}$$

根据引理2可知 b 对模 $G_{m_i}(i=1,2,\cdots,k)$ 的指数分别是 $2b^{m_i}(i=1,2,\cdots,k)$,故由引理1,从(11)式可得 $2b^{m_i}\mid d$,$i=1,2,\cdots,k$。又因

$$2b^{m_i}\mid 2b^{m_k},i=1,2,\cdots,k \tag{12}$$

所以条件(12)可写成

$$2b^{m_k}\mid d \tag{13}$$

另一方面,因为从引理2可知

$$b^{2b^{m_i}}\equiv 1(\mathrm{mod}\ G_{m_i}),i=1,2,\cdots,k \tag{14}$$

又从引理4可知 $G_{m_1},G_{m_2},\cdots,G_{m_k}$ 两两互素,所以根据引理3,从(10)、(12)和(14)式可得

$$b^{2b^{m_k}}\equiv 1(\mathrm{mod}\ n) \tag{15}$$

因此,根据引理1,从(15)式可知

$$d\mid 2b^{m_k} \tag{16}$$

于是,结合(13)、(16)式即得 $d=2b^{m_k}$。 证毕

证明 (定理2) 设 n 是适合(10)式。因为 $m_1<m_2<\cdots<m_k$,且 b 是偶数,故从(2)、(10)式可得

$$n=(b^{b^{m_1}}+1)(b^{b^{m_2}}+1)\cdots(b^{b^{m_k}}+1)=1+b^{b^{m_1}}t$$

其中 t 是适合 $gcd(t,b)=1$ 的正奇数。因此,整除关系

$$2b^{m_k}\mid(n-1) \tag{17}$$

成立的充要条件是

$$m_k\leqslant b^{m_1}-1 \tag{18}$$

另外,根据引理5可知 b 对模 n 的指数等于 $2b^{m_k}$,所以从引理1可知 n 是底为 b 的伪素数的充要条件是整除关系(17)式成立。因此,从前面的分析可知该充要条件可等价地表述为(18)式。 证毕

参考文献：

[1] Guy R K. Unsolved problems in number theory[M]. 3rd edition. Beijing: Science Press, 2007.

[2] 熊全淹. 初等整数论[M]. 武汉：湖北教育出版社，1985.
Xiong Q Y. Elementary integer arithmetic[M]. Wuhan: Hubei Education Publishing House, 1985.

[3] 潘承洞，潘承彪. 初等数论[M]. 北京：北京大学出版社，1992.
Pan C D, Pan C B. Elementary number theory[M]. Beijing: Peking University Press, 1992.

[4] 柯召，孙琦. 数论讲义(上册)[M]. 北京：高等教育出版社，1990.
Ke Z, Sun Q. Number theory handout [M]. Beijing: Higher Education Press, 1990.

[5] 蒙正中. 关于绝对伪素数的判别与计算[J]. 广西大学学报：自然科学版，2003，28(2)：125-128.
Meng Z Z. On the determination and calculation of carmicheal number[J]. Journal of Guangxi University: Natural Science Edition, 2003, 28(2): 125-128.

[6] 王云葵. 任何费马数都是素数或伪素数[J]. 玉林师范学院学报：自然科学版，1998(3)：26-28.
Wang Y K. Any Fermat number is a prime number or pseudo prime[J]. Journal of Yulin Normal University: Natural Science Edition, 1998(3): 26-28.

[7] 管训贵. 费马数与伪素数[J]. 四川理工学院报：自然科学版，2011，24(2)：140-141.
Guan X G. Fermat number and pseudo prime[J]. Journal of Sichuan Institute of Technology: Natural Science Edition, 2011, 24(2): 140-141.

[8] Cipolla M. Sui numeri composti P che verificiano Annali di Fermat $o^{p-1}\equiv 1 (\mathrm{mod}\ p)$[J]. Annali di Matematica, 1904, 9(2): 139-160.

[9] 闵嗣鹤，严士健. 初等数论[M]. 北京：高等教育出版社，2004 .
Min S H, Yan S J. Elementary integer arithmetic[M]. Beijing: Higher Education Press, 2004.

Generalized Fermat Numbers and Pseudoprimes

LIU Miao-hua, JIAO Hong-ying

(School of Science, Air Force Engineering University, Xi' an 710051, China)

Abstract: Let $G_m=b^{b^m}+1$, where b and m are positive integers with $2\mid b$. In this paper, using certain elementary methods, we prove that: i) G_m is either a prime or a pseudoprime to base b; ii) Let m_1, m_2, …, m_k be positive integers with $m_1<m_2<\cdots<m_k$. The product $G_{m_1}G_{m_2}\cdots G_{m_k}$ is a pseudoprime to base b if and only if $m_k\leqslant b^{m_1}-1$.

Keywords: generalized Fermat number; product; pseudoprime

(责任编辑 黄 颖)