Vol. 35 (2015)
No. 1

数 学 杂 志
J. of Math. (PRC)

奇完全数的两个性质

贺艳峰 [1] , 孙春丽 [2]
(1. 延安大学计算机学院, 陕西 延安 716000)
(2. 中共陕西省委党校, 陕西 西安 710061)

摘 要: 本文研究了奇完全数的两个性质. 利用初等的方法以及除数函数的性质对于 Jouchard [4] 提出的猜想给出了确切的证明, 并且推广 Yamada[5] 等人的结果.

关键词: 奇完全数; Euler 因子; 存在性
MR(2010) **主题分类号**: 11A25 **中图分类号**: O156.1
文献标识码: A **文章编号**: 0255-7797(2015)01-0135-06

1 引言及结论

对于正整数 n, 设 $\sigma(n)$ 是 n 的所有约数之和. 当 n 满足

$$\sigma(n) = 2n \tag{1.1}$$

时, n 称为完全数. 长期以来, 奇完全数的存在性及其相关问题一直是数论中引人关注的研究课题 [1]. 本文将运用初等的方法讨论奇完全数的两个性质.

早在十八世纪, Euler 曾经证明: 如果 n 是完全数, 则 n 必可表成

$$n = p^{\alpha} q_1^{2\beta_1} \cdots q_k^{2\beta_k}, \tag{1.2}$$

其中 $p, q_1, \cdots, q_k$ 是不同的奇素数, $\alpha, \beta_1, \cdots, \beta_k$ 是正整数, 而且 $p \equiv \alpha \equiv 1 \pmod 4$. 此时, (1.2) 式中的 p 称为奇完全数 n 的 Euler 因子. 本文将始终假定 n 是表成 (1.2) 式之形的奇完全数. 对此, Starni [2] 证明了: 当 $q_i \equiv -1 \pmod 4 (i = 1, \cdots, k)$ 时, $\frac{1}{2}\sigma(p^{\alpha})$ 必为合数. 最近, 朱玉扬 [3] 证明了: $n \not\equiv -1 \pmod 3$, 从而推出: 当 $q_i \equiv -1 \pmod 3 (i = 1, \cdots, k)$ 时, $\frac{1}{2}\sigma(p^{\alpha})$ 必为合数. 这里应该指出: 文献 [3] 的这一结果早已由 Touchard [4] 证明了. 同时, 文献 [3] 提出了以下猜想:

猜想 1.1 当 $q_i \equiv -1 \pmod m (i = 1, \cdots, k)$, 其中 m 是大于 2 的正整数时, $\frac{1}{2}\sigma(p^{\alpha})$ 必为合数.

本文完整地解决了猜想 1.1, 即证明了:

定理 1.1 对于任意大于 2 的正整数 m, 如果 $q_i \equiv -1 \pmod m (i = 1, \cdots, k)$, 则 $\frac{1}{2}\sigma(p^{\alpha})$ 必为合数.

*收稿日期: 2013-03-20 接收日期: 2013-04-28
基金项目: 陕西省科技厅项目基金资助 (2013JQ1019); 陕西省高水平大学建设专项基金资助项目基金资助 (2012SXTS07).
作者简介: 贺艳峰 (1976 –), 女, 陕西神木县, 讲师, 主要研究方向: 数论.

另外, Yamada [5] 讨论了适合条件 $\beta_1 = \beta_2 = \cdots = \beta_k = \beta$ 的奇完全数 n, 其中 β 是正整数. 文献 [5] 中证明了适合此条件的奇完全数 n 都满足 $n \leq 2^{4^\gamma}$, 其中 $\gamma = 4\beta^2 + 2\beta + 3$. 本文将证明当 $\beta \in \{1, 2\}$ 时, 不存在此类奇完全数, 即

定理 1.2 如果 $\beta_1 = \beta_2 = \cdots = \beta_k = \beta$, 则必有 $\beta \geq 3$.

由于运用定理 1.2 的证明方法, 可以通过计算得知: 对于很多正整数 β, 不存在适合条件 $\beta_1 = \beta_2 = \cdots = \beta_k = \beta$ 的奇完全数, 因此本文提出以下猜想:

猜想 1.2 不存在适合条件 $\beta_1 = \beta_2 = \cdots = \beta_k = \beta$ 的奇完全数 n.

2 定理 1.1 的证明

为了完成定理的证明, 我们首先引入如下的一个引理.

引理 2.1 [6] 如果 $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ 是 n 的标准分解式, 则

$$\sigma(n) = \prod_{i=1}^{r} \sigma(p_i^{\alpha_i}),$$

其中

$$\sigma(p_i^{\alpha_i}) = \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}, i = 1, \cdots, r.$$

定理 1.1 的证明 根据引理 2.1 可知, 当 n 是表成 (1.2) 式的奇完全数时, 从 (1.1) 式可得

$$\frac{1}{2}\sigma(p^\alpha) \prod_{i=1}^{s} \sigma(q_i^{2\beta_i}) = p^\alpha \prod_{i=1}^{s} q_i^{2\beta_i}. \tag{2.1}$$

因为 $p \equiv \alpha \equiv 1 \pmod 4$, 所以

$$\frac{1}{2}\sigma(p^\alpha) = (\frac{p+1}{2})(\frac{p^{\alpha+1} - 1}{p^2 - 1}), \tag{2.2}$$

其中 $(p+1)/2$ 和 $(p^{\alpha+1} - 1)/(p^2 - 1)$ 都是正奇数, 而且 $(p+1)/2 > 1$. 如果 $\frac{1}{2}\sigma(p^\alpha)$ 不是合数, 则从 (2.2) 式可知 $(p+1)/2$ 是奇素数, 且 $\alpha = 1$. 由于 $\gcd(p, (p+1)/2) = 1$, 故从 (2.1) 和 (2.2) 式可知

$$\frac{1}{2}\sigma(p^\alpha) = \frac{p+1}{2} = q_j, 1 \leq j \leq s. \tag{2.3}$$

当 $q_i \equiv -1 \pmod m (i = 1, 2, \cdots, s)$ 时, 从 (2.3) 式可知

$$p \equiv -3 \pmod m. \tag{2.4}$$

同时, 因为

$$q_i^{2\beta_i} \equiv 1 \pmod m, \ \sigma(q_i^{2\beta_i}) = 1 + q_i + \cdots + q_i^{2\beta_i} \equiv 1 \pmod m, i = 1, 2, \cdots, s. \tag{2.5}$$

所以从 (2.1), (2.3) 和 (2.4) 式可得

$$-1 \equiv q_j \equiv \frac{1}{2}\sigma(p^\alpha) \prod_{i=1}^{s} \sigma(q_i^{2\beta_i}) \equiv p^\alpha \prod_{i=1}^{s} q_i^{2\beta_i} \equiv p \pmod m. \tag{2.6}$$

结合 (2.4) 和 (2.6) 式, 即得 $2 \equiv 0 \pmod{m}$. 然而, 由于 $m > 2$, 故不可能. 由此可知 $\frac{1}{2}\sigma(p^\alpha)$ 必为合数. 定理证毕.

3 定理 1.2 的证明

为了完成定理的证明, 我们需要如下的六个引理.

引理 3.1 [7] 设 l 是奇素数, X 和 Y 是适合 $X > Y$ 以及 $\gcd(X, Y) = 1$ 的正整数, 又设 q 是 $(X^l - Y^l)/(X - Y)$ 的素因数. 此时, $q = l$ 或者 $q \equiv 1 \pmod{2l}$; $l \mid (X^l - Y^l)/(X - Y)$ 成立的充要条件是 $X \equiv Y \pmod{l}$, 而且此时 $l \parallel (X^l - Y^l)/(X - Y)$.

引理 3.2 [8] 方程

$$\frac{X^m - 1}{X - 1} = Y^2, \quad X, Y, m \in \mathbb{N}, \quad \min\{X, Y, m\} > 1$$

仅有解 $(X, Y, m) = (3, 11, 5)$ 和 $(7, 20, 4)$.

引理 3.3 [9] 如果 n 是适合 (1.2) 式的奇完全数, 则 $k \geq 8$.

引理 3.4 当 $\beta_1 = \beta_2 = \cdots = \beta_k = \beta$ 时, 如果 $l = 2\beta + 1$ 是奇素数, 则

$$n = p^\alpha (l f_1 \cdots f_r g_1 \cdots g_s)^{l-1}, \tag{3.1}$$

其中 $f_i (i = 1, \cdots, r)$ 是适合 $f_i \equiv 1 \pmod{l}$ 的奇素数, $g_j (j = 1, \cdots, s)$ 是适合 $g_j \not\equiv 0, 1 \pmod{l}$ 的奇素数, 而且 $1 \leq r \leq l - 1$.

证 当 $\beta_1 = \beta \cdots = \beta_k = \beta$ 且 $l = 2\beta + 1$ 是奇素数时, 从 (1.2) 式可得

$$n = p^\alpha (q_1 \cdots q_k)^{l-1}, \tag{3.2}$$

根据引理 2.1, 从 (1.1) 和 (3.2) 式可知

$$\sigma(n) = \frac{p^{\alpha+1} - 1}{p - 1} \prod_{i=1}^{k} \frac{q_i^l - 1}{q_i - 1} = 2p^\alpha (q_1 \cdots q_k)^{l-1}. \tag{3.3}$$

因为 $p \equiv \alpha \equiv 1 \pmod{4}$, 故有

$$2 \parallel \frac{p^{\alpha+1} - 1}{p - 1}, \quad \gcd(p^\alpha, \frac{p^{\alpha+1} - 1}{p - 1}) = 1. \tag{3.4}$$

如果 $q_i \not\equiv 1 \pmod{l} (i = 1, \cdots, k)$, 则从引理 3.1 可知

$$\gcd(q_1 \cdots q_k, \prod_{i=1}^{k} \frac{q_i^l - 1}{q_i - 1}) = 1. \tag{3.5}$$

因此, 从 (3.3), (3.4) 和 (3.5) 式可得

$$\frac{p^{\alpha+1} - 1}{p - 1} = 2(q_1 \cdots q_k)^{l-1} \tag{3.6}$$

以及

$$\prod_{i=1}^{k} \frac{q_i^l - 1}{q_i - 1} = p^\alpha. \tag{3.7}$$

当 $\alpha=1$ 时, 因为 $(q_i^l-1)/(q_i-1)>1(i=1,2,\cdots,k)$, 又从引理 3.3 可知 $k\geq 8$, 所以 (3.7) 式不可能成立. 因此 $\alpha>1$.

当 $\alpha>1$ 时, 由于 $(p^{\alpha+1}-1)/(p-1)=(p^{(\alpha+1)/2}+1)(p^{(\alpha+1)/2}-1)/(p-1), 2\parallel(p^{(\alpha+1)/2}+1)$ 且 $\gcd(p^{(\alpha+1)/2}+1,(p^{(\alpha+1)/2}-1)/(p-1))=1$, 故从 (3.6) 式可得 $p^{(\alpha+1)/2}+1=2u^{l-1}$ 和

$$\frac{p^{(\alpha+1)/2}-1}{p-1}=v^{l-1}, \tag{3.8}$$

其中 u,v 是适合 $uv=q_1\cdots q_k$ 的正整数. 因为 $(\alpha+1)/2$ 是大于 1 的奇数, $l-1$ 是偶数, 所以根据引理 3.2, 从 (3.8) 式可知 $p=3$, 与 $p\equiv 1 \pmod 4$ 矛盾. 由此可知 $q_1,\cdots,q_k$ 中必有某个素数 q 适合 $q\equiv 1 \pmod l$. 由于从引理 3.1 可知此时 $l\mid(q^l-1)/(q-1)$, 故从 (3.3) 式可得

$$l\in\{p,q_1,\cdots,q_k\}. \tag{3.9}$$

如果 $p=l$, 则 $q_i\neq l(i=1,\cdots,k)$. 因为 l 是奇素数, 所以根据 Euler 定理可知 $q_i^{l-1}\equiv 1 \pmod l(i=1,\cdots,k)$, 故有

$$(q_1\cdots q_k)^{l-1}\equiv 1 \pmod l. \tag{3.10}$$

另外, 从引理 3.1 可知

$$\begin{cases} \dfrac{q_j^l-1}{l(q_j-1)}\equiv 1 \pmod l, & \text{当 } q_j\equiv 1 \pmod l \text{ 时;} \\ \dfrac{q_j^l-1}{q_j-1}\equiv 1 \pmod l, & \text{当 } q_j\not\equiv 1 \pmod l \text{ 时,} \end{cases} \quad 1\leq j\leq k. \tag{3.11}$$

因此, 从 (3.3), (3.10) 和 (3.11) 式可得

$$\begin{aligned} 2\equiv 2(q_1\cdots q_k)^{l-1}&\equiv\Big(\frac{p^{\alpha+1}-1}{p-1}\Big)\Big(\frac{1}{p^\alpha}\prod_{i=1}^{k}\frac{q_i^l-1}{q_i-1}\Big) \\ &\equiv\Big(\frac{l^{\alpha+1}-1}{l-1}\Big)\Big(\frac{1}{l^\alpha}\prod_{i=1}^{k}\frac{q_i^l-1}{q_i-1}\Big)\equiv 0\text{或}1 \pmod l \end{aligned} \tag{3.12}$$

这是一个矛盾. 由此可知 $p\neq l$, 故从 (3.9) 式可知 $l\in\{q_1,\cdots,q_k\}$. 因此, 从 (3.2) 式可知, 此时 n 可表成 (3.1) 式之形.

根据引理 2.1, 从 (1.1) 和 (3.1) 式可得

$$\begin{aligned} \sigma(n)=&\Big(\frac{p^{\alpha+1}-1}{p-1}\Big)\Big(\frac{l^l-1}{l-1}\Big)\Big(\prod_{i=1}^{r}\frac{f_i^l-1}{f_i-1}\Big)\Big(\prod_{j=1}^{s}\frac{g_j^l-1}{g_j-1}\Big) \\ =&2p^\alpha(lf_1\cdots f_rg_1\cdots g_s)^{l-1}. \end{aligned} \tag{3.13}$$

因为 $f_i\equiv 1 \pmod l(i=1,\cdots,r)$, 所以 $l\mid(f_i^l-1)/(f_i-1)(i=1,\cdots,r)$. 于是从 (3.13) 式可知 $r\leq l-1$. 引理证毕.

引理 3.5 [10] 方程

$$X^2+X+1=Y^m, X,Y,m\in\mathbb{N},\quad X>1,Y>1,m>2 \tag{3.14}$$

没有适合 $3\nmid m$ 的解 (X,Y,m).

引理 3.6. [11] 方程 (3.14) 仅有解 $(X,Y,m)=(18,7,3)$ 适合 $3\mid m$.

定理 1.2 的证明 首先考虑 $\beta=1$ 的情况. 因为此时 $l=2\beta+1=3$ 是奇素数, 所以根据引理 3.4, 从 (3.1) 和 (3.13) 式分别可得

$$n=p^{\alpha}(3f_1\cdots f_rg_1\cdots g_s)^2 \tag{3.15}$$

和

$$\begin{aligned}&\big(\frac{p^{\alpha+1}-1}{p-1}\big)(3^2+3+1)\big(\prod_{i=1}^{r}(f_i^2+f_i+1)\big)\big(\prod_{j=1}^{s}(g_j^2+g_j+1)\big)\\ =&2p^{\alpha}(3f_1\cdots f_rg_1\cdots g_s)^2,\end{aligned} \tag{3.16}$$

其中 $r\le 2$. 由于 $g_j\not\equiv 0$或$1 \pmod 3$, 所以根据引理 3.1, 从 (3.16) 式可得

$$(3^2+3+1)\big(\prod_{i=1}^{r}\frac{1}{3}(f_i^2+f_i+1)\big)\big(\prod_{j=1}^{s}(g_j^2+g_j+1)\big)\mid p^{\alpha}f_1^2\cdots f_r^2. \tag{3.17}$$

然而, 因为 $r\le 2,(f_i^2+f_i+1)/3>1(i=1,\cdots,r),g_j^2+g_j+1>1(j=1,\cdots,s)$, 而且, 从引理 3.3 可知 $r+s=k-1\ge 7$, 所以根据引理 3.5 和 3.6 可知 (3.17) 式不可能成立. 因此, 当 $\beta=1$ 时, n 不是完全数.

以下考虑 $\beta=2$ 的情况. 此时,

$$n=p^{\alpha}(5f_1\cdots f_rg_1\cdots g_s)^4, \tag{3.18}$$

$$\begin{aligned}\sigma(n)&=\big(\frac{p^{\alpha+1}-1}{p-1}\big)\big(\frac{5^5-1}{5-1}\big)\big(\prod_{i=1}^{r}\frac{f_i^5-1}{f_i-1}\big)\big(\prod_{j=1}^{s}\frac{g_j^5-1}{g_j-1}\big)\\ &=2p^{\alpha}(5f_1\cdots f_rg_1\cdots g_s)^4,\end{aligned} \tag{3.19}$$

其中 $r\le 4$, 因为 $(5^5-1)/(5-1)=11\times 71$, 而且素数 11 和 71 适合 $11\equiv 71\equiv 3 \pmod 4$, 所以 Euler 因子 $p\not\equiv 11$或71, 故从 (3.19) 式可知

$$\{11,71\}\subseteq\{f_1,\cdots,f_r\}. \tag{3.20}$$

又因 $(11^5-1)/(11-1)=5\times 3221,(71^5-1)/(71-1)=5\times 11\times 211\times 2221$, 其中 $2111\equiv 3 \pmod 4$, 故从 (3.19) 式可知 $211\in\{f_1,\cdots,f_r\}$, 而且素数 2221 和 3221 中至少有一个数属于 $\{f_1,\cdots,f_r\}$. 再因

$$\gcd(11\times 71\times 2221\times 3221,(211^5-1)/(211-1))=1,$$

故从 (3.20) 式可得 $r\ge 5$ 这一矛盾. 由此可知: 当 $\beta=2$ 时, n 也不是完全数. 定理证毕.

参 考 文 献

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

[2] Starni P. On the Euler's factor of an odd perfect number[J]. J. Number Theory, 1991, 37(3): 366–369.

[3] Zhu Y Y. Several results on odd perfect numbers [J]. Adv. Math. China, 2011, 40(5): 595–598 (in Chinese).

[4] Touchard J. On prime numbers and perfect numbers[J]. Scripta Math., 1953, 19(1): 35–39.

[5] Yamada T. Odd perfect numbers of a special form [J]. Colloq. Math., 2005, 103(2): 303–307.

[6] Hua L -G. Introduction to number theory[M]. Beijing: Science Press, 1979.

[7] Möller K. Untere Schranke für die Anzahl der Primzahlen, aus denen x, y, z der Fermatschen Geichung $x^n + y^n = z^n$ bestehen muss [J]. Math. Nachr., 1955, 14(1): 25–28.

[8] Ljunggren W. Noen setninger om ubestemte likninger av formen $(x^n - 1)/(x - 1) = y^q$ [J]. Norsk. Mat. Tidsskr., 1943, 25(1): 17–20.

[9] Nielsen P P. Odd perfect numbers have at least nine distinct prime factors [J]. Math. Comput., 2007, 76(260): 2109–2126.

[10] Nagell T. Des equations indéterminées $x^2+x+1 = y^n$ et $x^2+x+1 = 3y^n$ [J]. Norsk. Mat. Forenings Skrifter, Ser. 1, 1921,(2): 14.

[11] Ljunggren W. Einige bemerkungen über die darstellung ganzer Zahlen durch binare kubische Formenmir positiver diskriminante [J]. Acta Math., 1942, 75(1): 1–21.

TWO PROPERTIES OF ODD PERFECT NUMBERS

HE Yan-feng[1] , SUN Chun-li[2]

(*1.College of Mathematics and Computer Science, Yan'an University, Yan'an 716000, China*)

(*2. Shaanxi Province Committee Party School of the Chinese Communist, Xi'an 710061, China*)

Abstract: In this paper, we study two properties of the odd perfect number. By using the elementary method and the properties of the divisor function, we give an explicit proof for the conjecture which was proposed by Touchard [4], which improvers the result of Yamada in [5].

Keywords: odd perfect number; Euler factor; existence

2010 MR Subject Classification: 11A25