

关于方程 $X^2 = Dy^4 + 4$

李 晓 莲

(基础课部)

摘要 本文进一步研究了方程 $x^2 = Dy^4 + 4$ ($D > 0$ 且不为平方数) 的正整数解, 得到了如下结果: 设对 D 的任一分解 $D = mn$, $m > 1$, $n > 1$, 均有 $(m/n) = -1$, 此处 (m/n) 表示 Jacobi 符号。如果 (1) D 含有 $4k+3$ 的因子, 或 (2) $D \equiv 13 \pmod{16}$, 或 (3) $(m, n) \equiv (1, 5) \pmod{16}$ 或 $(m, n) \equiv (5, 1) \pmod{16}$, 则方程 $x^2 = Dy^4 + 4$ 均无奇数解。

主题词 分解; 模; 素数; 正整数; 雅可比符号; 奇数解; 平方数; 奇素数; 素因子。

方程

$$x^2 = Dy^4 + 4, D > 0 \text{ 且不为平方数} \quad (1)$$

为一著名的二元四次丢番图方程, 国内外对此有过许多研究, 例如, Cohn^[1] 曾经证明了: 如果 D 使方程 $X^2 - Dy^2 = -4$ 有奇数解 $X \equiv Y \equiv 1 \pmod{2}$, 则方程 (1) 除 $D = 5$ 时仅有解 $(x, y) = (3, 1)$ 和 $(322, 12)$ 外, 无其它正整数解。

由于方程 (1) 如有偶数解时可化为方程 $x_1^2 - D_1 y_1^4 = 1$, 对后者已有许多讨论, 因此, Velupillai^[2] 对方程 (1) 的奇数解进行了研究。例如, 他给出了当 $D \leq 181$ 时方程 (1) 的全部解。此后, 曹珍富^{[3][4]} 对方程 (1) 有过较系统的研究, 得出了带有一般性的结果。

本文进一步研究了方程 (1) 的正整数解, 得到了如下结果:

定理 设对 D 的任一分解 $D = mn$, $m > 1$, $n > 1$ 均有 $(m/n) = -1$, 此处 (m/n) 表示 Jacobi 符号, 如果

1) D 含有 $4k+3$ 的因子, 或 2) $D \equiv 13 \pmod{16}$; 或 3) $(m, n) \equiv (1, 5) \pmod{16}$ 或 $(m, n) \equiv (5, 1) \pmod{16}$; 则方程 (1) 均无奇数解。

证 先将方程 (1) 改写成

$$(x+2)(x-2) = Dy^4 \quad (2)$$

假设方程 (1) 有奇数解 x, y , 则有 $2/x$, 故 $(x+2, x-2) = 1$, 于是 (2) 式给出

$$x \pm 2 = y_1^4, x \mp 2 = Dy_2^4, y = y_1 y_2 \quad (3)$$

或

$$x+2 = my_1^4, x-2 = ny_2^4, y = y_1 y_2 \quad (4)$$

其中 $D = mn$, $m > 1$, $n > 1$ 为 D 的任一分解。

首先将 (4) 式中的前两式相减得

$$4 = my_1^4 - ny_2^4$$

对上式取模 n 得 $my_1^4 \equiv 4 \pmod{n}$, 因此 $(my_1^2)^2 \equiv 4m \pmod{n}$, 因 $(m/n) = -1$, 故有 $(m, n) = 1$, 令 $n = p_1 p_2 \cdots p_s$, $p_i (i = 1, 2, \dots, s)$ 为奇素数, 则 $(4m/p_i) = 1$, 即 $(m/p_i) = 1$, 由此,
$$\left(\frac{m}{n}\right) = \prod_{i=1}^s (m/p_i) = 1,$$
 比与假定 $(m/n) = -1$ 矛盾, 故(4)式为不可能。

其次将(3)式中的前两式相减得

$$4 = y_1^4 - Dy_2^4 \quad (5)$$

或

$$-4 = y_1^4 - Dy_2^4 \quad (6)$$

先讨论方程(5), 将它改写成

$$(y_1^2 - 2)(y_1^2 + 2) = Dy_2^4 \quad (7)$$

因 $y = y_1 y_2$ 为奇数, 故 $2/y_1$, 由此, $(y_1^2 + 2, y_1^2 - 2) = 1$, 故由(7)式给出

$$y_1^2 \pm 2 = a^4, \quad y_1^2 \mp 2 = Db^4, \quad y_2 = ab \quad (8)$$

或

$$y_1^2 + 2 = ma^4, \quad y_1^2 - 2 = nb^4, \quad y_2 = ab \quad (9)$$

其中 $D = mn$, $m > 1$, $n > 1$ 为 D 的任一分解, 因为任意两正整数的平方之差不等于 2, 故(8)式不可能成立。又将(9)式中的前两式相减得

$$4 = ma^4 - nb^4$$

对上式取模 n 便得 $ma^4 \equiv 4 \pmod{n}$, 故又得 $(m/n) = 1$, 此与假定 $(m/n) = -1$ 矛盾, 故(9)式不可能成立, 这就说明方程(5)不能成立。

再讨论方程(6), 将它改写成

$$y_1^4 + 4y_1^2 + 4 - 4y_1^2 = Dy_2^4$$

即

$$(y_1^2 + 2y_1 + 2)(y_1^2 - 2y_1 + 2) = Dy_2^4 \quad (10)$$

现在证明 $(y_1^2 + 2y_1 + 2, y_1^2 - 2y_1 + 2) = 1$ 。设 $(y_1^2 + 2y_1 + 2, y_1^2 - 2y_1 + 2) = d$, 记 $y_1^2 + 2y_1 + 2 = ds$, $y_1^2 - 2y_1 + 2 = dt$, $(s, t) = 1$, 则 $4y_1 = d(s - t)$, $2(y_1^2 + 2) = d(s + t)$, 因 y_1 为奇数, 故 $2 \nmid d$, 由此, d/y_1 , $d/y_1^2 + 2$, 所以 $d/(y_1, y_1^2 + 2)$, 但 y_1 为奇数, 故有 $(y_1, y_1^2 + 2) = 1$, 因而 $d/1$, 即 $d = 1$, 于是由(10)式给出

$$y_1^2 \pm 2y_1 + 2 = a^4, \quad y_1^2 \mp 2y_1 + 2 = Db^4, \quad y_2 = ab \quad (11)$$

或

$$y_1^2 + 2y_1 + 2 = ma^4, \quad y_1^2 - 2y_1 + 2 = nb^4, \quad y_2 = ab \quad (12)$$

其中 $D = mn$, $m > 1$, $n > 1$ 为 D 的任一分解。

将(11)式中第一式改写成 $(y_1 \pm 1)^2 + 1 = a^4$, 若 $y_1 = 1$, 由(11)式的第二式知 $Db^4 = 1$ 或 5, 此不可能, 由此 $y_1 > 1$, 故 $y_1 \pm 1 > 0$, 但任意两正整数的平方差不可能等于 1, 故(11)式不可能成立。

现在讨论(12)式:

1) 当 D 含有 $4k + 3$ 的因子时, 不妨设 $p = 4k + 3$, 则 p/m 或 p/n , 若 p/m , 由(12)式的第一式得

$$(y_1 + 1)^2 + 1 = ma^4, p/m,$$

对上式取模 p 得 $(y_1 + 1)^2 \equiv -1 \pmod{p}$, 但 $p \equiv 3 \pmod{4}$, $(-1/p) = -1$, 故此为不可能。同理, 若 p/n , 则由(12)式的第二式得 $(y_1 - 1)^2 + 1 = nb^4$, 对此式取模 p 得 $(y_1 - 1)^2 \equiv -1 \pmod{p}$, 此亦为不可能。

2) 当 $D \equiv 13 \pmod{16}$ 时, 由1)的讨论知, 可设 D 不含形为 $4k+3$ 的因子, 故对 D 的任一分解 $D = mn, m > 1, n > 1$, 有

$$(i) m \equiv 1 \pmod{16}, n \equiv 13 \pmod{16};$$

$$(ii) m \equiv 5 \pmod{16}, n \equiv 9 \pmod{16};$$

$$(iii) m \equiv 9 \pmod{16}, n \equiv 5 \pmod{16};$$

$$(iv) m \equiv 13 \pmod{16}, n \equiv 1 \pmod{16}.$$

不论哪种情形都有 $m + n \equiv 14 \pmod{16}$, 现将(12)式的前两式相加得

$$2(y_1^2 + 2) = ma^4 + nb^4 \quad (13)$$

由于 y_1, a, b 均为奇数, 易知

$$y_1^2 \equiv 1 \pmod{8}, 2(y_1^2 + 2) \equiv 6 \pmod{16},$$

$$a^4 \equiv 1 \pmod{16}, b^4 \equiv 1 \pmod{16}$$

故对(13)式取模16便得 $m + n \equiv 6 \pmod{16}$, 此与上述所得 $m + n \equiv 14 \pmod{16}$ 矛盾。

3) 当 $D = mn, m > 1, n > 1$ 为 D 的任一分解时, 若 $m \equiv 1 \pmod{16}$, 现在利用(12)证明 $n \equiv 5 \pmod{16}$ 。

显然, 由 $m > 1, n > 1$, 故(12)式给出 $y_1 > 1$, 对(12)式的第一式取模 y_1 得

$$ma^4 \equiv 2 \pmod{y_1}.$$

因 y_1 为奇数, 但易知 $(a^4, y_1) = 1$, 故

$$(2/y_1) = (ma^4/y_1) = (m/y_1).$$

另一方面, 由(12)式前两式相减得

$$4y_1 = ma^4 - nb^4 \quad (14)$$

由1)的讨论, 可设 $D = mn$ 不含形 $4k+3$ 的因子, 但 $2 \nmid D$, 故 D 的素因子均为 $4k+1$ 形, 但任意两个 $4k+1$ 形之数相乘其积亦为 $4k+1$ 形, 故得

$$m \equiv 1 \pmod{4}, n \equiv 1 \pmod{4}.$$

对(14)式取模 m 得 $4y_1 \equiv -nb^4 \pmod{m}$, 设 $m = q_1 q_2 \cdots q_t$, $q_i (i = 1, 2, \dots, t)$ 为奇素数, 因 $(4, q_i) = 1$, 故 $(y_1/q_i) = (4y_1/q_i) = (-n/q_i)$, 由此得

$$\left(\frac{y_1}{m}\right) = \prod_{i=1}^t \left(\frac{y_1}{q_i}\right) = \prod_{i=1}^t \left(\frac{-n}{q_i}\right) = \left(\frac{-n}{m}\right).$$

又 $m \equiv 1 \pmod{4}, n \equiv 1 \pmod{4}$, 则有

$$\left(\frac{-1}{m}\right) = 1, (n/m) = (m/n)$$

于是 $(y_1/m) = (-n/m) = (-1/m)(n/m) = (n/m) = (m/n) = -1$,

再由前面所得 $(2/y_1) = (m/y_1)$ 可知

$$(2/y_1 = (m/y_1) = (y_1/m) = -1.$$

但 $(2/y_1) = (-1)^{(y_1^2-1)/8}$, 故必 $y_1 \equiv \pm 3 \pmod{8}$ 。

下面证明 $y_1 \equiv -3 \pmod{8}$, 由于 $m \equiv 1 \pmod{16}$ 及 $a^4 \equiv 1 \pmod{16}$, 故由(12)式的第一式知 $y_1^2 + 2y_1 + 2 \equiv 1 \pmod{16}$, 即 $(y_1 + 1)^2 \equiv 0 \pmod{16}$, 由此易知 $y_1 + 1 \equiv 0 \pmod{4}$, 因此从 $y_1 \equiv \pm 3 \pmod{8}$ 只能有

$$y_1 \equiv 3 \pmod{8}.$$

现由(12)式的第二式取模16得 $9 - 6 + 2 \equiv n \pmod{16}$, 即 $n \equiv 5 \pmod{16}$ 。

同理, 若 $m \equiv 5 \pmod{16}$, 则由(12)式可得 $n \equiv 1 \pmod{16}$ 。

当 $m \equiv 9 \pmod{16}$ 或 $m \equiv 13 \pmod{16}$ 时, 从(12)式可分别有 $(y_1 + 1)^2 \equiv 8 \pmod{16}$ 或 $(y_1 + 1)^2 \equiv 12 \pmod{16}$, 即 $(y_1 + 1/2)^2 \equiv 2 \pmod{4}$ 或 $(y_1 + 1/2)^2 \equiv 3 \pmod{4}$, 但 y_1 为奇数, 此均为不可能证毕。

注: 关于方程(1)的奇数解, Velupillai对 $D = p$ (奇素数)时已在[2]中给出了解答; 而当 $D = pq$, (p, q 为不同的奇素数)时, 文[3]、[4]中得到了若干结果, 但这里作为定理的推论给出如下进一步的结果。

推论 设 $D = pq$, p, q 为不同的奇数, 且 $(q/p) = -1$, 则当下列六种情形中的任一种出现时, 方程(1)均无奇数解:

- 1) $p \equiv 1 \pmod{4}, q \equiv 3 \pmod{4}$;
- 2) $pq \equiv 13 \pmod{16}$;
- 3) $p \equiv 1 \pmod{16}, q \equiv 5 \pmod{16}$;
- 4) $p \equiv 5 \pmod{16}, q \equiv 1 \pmod{16}$;
- 5) $p \equiv 9 \pmod{16}$;
- 6) $p \equiv 13 \pmod{16}$ 。

证 1) 因 $D = pq, q \equiv 3 \pmod{4}$, 故由定理证明中的1)可知此时推论成立。

2) 利用定理证明中的2)即得。

3)~6) 利用定理证明中的3)即得。

最后指出, 在本文定理的类似条件下, 可以研究方程

$$x^2 - 4Dy^4 = 1$$

的解, 若能证明此方程对某些 D 无解, 则此时方程(1)就无偶数解。因此方程(1)的求解问题有可能对很大一类 D 得以解决。

参 考 文 献

- 1 Cohn J H E. Eight Diophantine equations. Proc. Land Math Soc, 1966, 16: 153~166
- 2 Velupillai M. The Diophantine equation $Y^2 = DX^4 + 4$. Bull Cal Math Soc, 1976, 68: 275~278
- 3 曹珍富. 关于丢番图方程 $X^2 = DY^4 + 4$. 哈尔滨工业大学科学研究报告, 1982, 235: 8~9
- 4 戴宗恕. 曹珍富. 关于丢番图方程 $X^2 = DY^4 + 4$ (II). 哈尔滨工业大学科学研究报告, 1982, 253: 10
- 5 华罗庚. 数论导引. 科学出版社, 1957

On the Equation $X^2 = Dy^4 + 4$

Li Xiaolian

Abstract: In this paper, the author further studies the positive integer solution of the equation $x^2 = Dy^4 + 4$ ($D > 0$ is not square number). The main result is as follows: For any decomposition $D = mn$ of D , there is $(m/n) = -1$, Where $m > 1$, $n > 1$, (m/n) represents Jacobi symbol. If (1) D contains a factor of the form $4k+3$, or (2) $D \equiv 13 \pmod{16}$, or (3) $(m, n) \equiv (1, 5) \pmod{16}$, or $(m, n) \equiv (5, 1) \pmod{16}$, then the equation $x^2 = Dy^4 + 4$ has no odd number solution.

Subject words: Decomposition; module; prime number; Positive integer solution; Jacobi symbol; odd number solution; square number; odd prime number; prime factor