

# 关于 Diophantine 方程 $x^3 \pm 1 = Dy^2$

梁 勇, 韩云娜

(西北大学数学系, 西安 710127)

**摘 要:** 利用数论中的同余, 勒让德符号的性质及其它一些方法, 研究丢番图方程  $x^3 \pm 1 = Dy^2$  ( $D = D_1 p$ ,  $D$  是无平方因子的正整数, 其中  $D_1$  是不能被 3 或  $6k + 1$  之形的素数整除的正整数,  $p = 3(12r + 7)(12r + 8) + 1$ ,  $r$  是正整数) 的解的情况。证明了当  $D_1 \equiv 7 \pmod{12}$  时, 方程  $x^3 + 1 = Dy^2$  无正整数解; 当  $D_1 \equiv 5 \pmod{8}$  时, 方程  $x^3 - 1 = Dy^2$  无正整数解。

**关键词:** 丢番图方程; 同余; 正整数解; Legendre 符号

**中图分类号:** O156.1

**文献标识码:** A

## 引 言

设  $N$  是全体正整数的集合,  $D$  是无平方因子的正整数。不定方程

$$x^3 \pm 1 = Dy^2, x, y \in N \quad (1)$$

是一类基本而又重要的三次 Diophantine 方程, 已有不少研究成果<sup>[1-2]</sup>, 柯召和孙琦<sup>[2]</sup>证明了: 当  $D$  大于 2 且不含  $6k + 1$  形的素因子时, 方程 (1) 无解。但当  $D$  含有  $6k + 1$  形的素因子时, 方程的求解比较困难, 段辉明<sup>[3]</sup>总结了:  $0 < D < 100$  时, 方程  $x^3 - 1 = Dy^2$  的解的情况。彭成刚<sup>[4]</sup>证明了:  $x^3 + 1 = 129y^2$  仅有非平凡解  $(80 \pm 63)$ 。乐茂华<sup>[5]</sup>证明了: 当  $p = 12r^2 + 1$ , 其中  $r$  是奇数, 则方程  $x^3 + 1 = py^2$  无正整数解  $(x, y)$ 。在此基础上, 本文推广了张淑静<sup>[6]</sup>相应的结论。

## 1 主要结果

**定理 1** 设  $D = D_1 p$ , 其中  $D$  是无平方因子正整数,  $D_1$  不能被 3 或  $6k + 1$  之形的素数整除,  $p$  是奇素数,  $p = 3(12r + 7)(12r + 8) + 1$ ,  $r$  是正整数, 则

(1) 当  $D_1 \equiv 7 \pmod{12}$  时, 方程

$$x^3 + 1 = Dy^2, x, y \in N \quad (2)$$

无解。

(2) 当  $D_1 \equiv 5 \pmod{8}$  时, 方程

$$x^3 - 1 = Dy^2, x, y \in N \quad (3)$$

无解。

为了证明定理 1, 先引入引理。

**引理 1** (1) 设  $D = D_1 D_2$ ,  $D_1$  不含  $6k + 1$  形的素因子,  $D_2$  仅含  $6k + 1$  形的素因子, 则方程  $x^3 \pm 1 = Dy^2$  有非平凡整数解的必要条件是存在某个  $(p, q)$  使方程

$$x \pm 1 = D_1 qa^2, x^2 \mp x + 1 = pb^2, y = ab \quad (4)$$

或

$$x \pm 1 = 3D_1 qa^2, x^2 \mp x + 1 = 3pb^2, y = 3ab \quad (5)$$

有解, 这里  $p > 0, q > 0, pq = D_\infty$ 。

(2) 当  $D > 2, p = 1$  时, (4) 式和 (5) 式均无非平凡解。

其证明参见文献 [7] 的性质 1 和文献 [8] 的性质 2。

## 2 定理的证明

**定理 1(1) 的证明,** 设  $(x, y)$  是方程 (2) 的解, 由于  $D_1$  不能被 3 或  $6k + 1$  之形的素数整除,  $p = 3(12r + 7)(12r + 8) + 1$  故根据引理 1 中的 (1), 方程 (2) 有 4 种可能的分解:

$$(I) x + 1 = D_1 pa^2, x^2 - x + 1 = b^2, y = ab \quad (6)$$

$$(II) x + 1 = D_1 a^2, x^2 - x + 1 = pb^2, y = ab \quad (7)$$

$$(III) x + 1 = 3D_1 pa^2, x^2 - x + 1 = 3b^2, y = 3ab \quad (8)$$

$$(IV) x + 1 = 3D_1 a^2, x^2 - x + 1 = 3pb^2, y = 3ab \quad (9)$$

情形 (I) 和 (III), 可由引理 1 中 (2) 知其不成立。

情形 (II), 由  $D_1 \equiv 7 \pmod{12}$  和 (7) 式的前式可得

$$x \equiv D_1 a^2 - 1 \equiv \begin{cases} 2 \pmod{4}, & \text{当 } a \text{ 为奇数时} \\ 3 \pmod{4}, & \text{当 } a \text{ 为偶数时} \end{cases}$$

所以

$$x^2 - x + 1 \equiv \begin{cases} 3 \pmod{4}, & \text{当 } a \text{ 为奇数时} \\ 3 \pmod{4}, & \text{当 } a \text{ 为偶数时} \end{cases} \quad (10)$$

由(7)式的后式得  $2 \nmid p b^2$ , 故  $2 \nmid b^2$ , 所以  $b^2 \equiv 1 \pmod{4}$ ,

$$\text{而 } p = 3(12r + 7)(12r + 8) + 1$$

因此

$$p b^2 \equiv 1 \pmod{4} \quad (11)$$

而  $x^2 - x + 1 \equiv p b^2 \pmod{4}$ , 所以(10)式和(11)式矛盾, 所以情形(II)不成立。

情形(IV), 由(9)式可得

$$3(2D_1 a^2 - 1)^2 + 1 = p(2b)^2 \quad (12)$$

从(12)式可知  $(X, Y) = (2b, 2D_1 a^2 - 1)$  是方程

$$pX^2 - 3Y^2 = 1, X, Y \in N^+ \quad (13)$$

的一组解, 因为  $p = 3(12r + 7)(12r + 8) + 1$ , 所以方程(13)的最小正整数解  $(X_1, Y_1) = (2, 24r + 15)$ , 于是根据文献[9]的结果可得

$$2b\sqrt{p} + (2D_1 a^2 - 1)\sqrt{3} = (2\sqrt{p} + (24r + 15)\sqrt{3})^t \quad (14)$$

其中  $t$  是正奇数。

由(14)式得  $2D_1 a^2 - 1 \equiv 0 \pmod{(24r + 15)}$ , 即

$$2D_1 a^2 - 1 \equiv 0 \pmod{3}, 4D_1^2 a^2 \equiv 2D_1 \pmod{3}, \text{ 因此}$$

$$\left(\frac{2D_1}{3}\right) = 1, \text{ 其中 } \left(\frac{2D_1}{3}\right) \text{ 表示模的勒让德符号, 然而, 由}$$

$$D_1 \equiv 7 \pmod{12} \text{ 得 } D_1 \equiv 1 \pmod{3}, \text{ 故}$$

$$\left(\frac{2D_1}{3}\right) = \left(\frac{2}{3}\right)\left(\frac{D_1}{3}\right) = \left(\frac{2}{3}\right)\left(\frac{1}{3}\right) = -1$$

矛盾。故情形(IV)不成立。

综上所述, 方程(2)在题设条件下无解。

定理 1(2)的证明, 设  $(x, y)$  是方程(3)的解, 根据

引理, 方程(3)可分解为两种情形:

$$(I) x - 1 = D_1 a^2, x^2 + x + 1 = p b^2, y = ab \quad (15)$$

$$(II) x - 1 = 3D_1 a^2, x^2 + x + 1 = 3p b^2, y = 3ab \quad (16)$$

情形(I), 由(15)式的前式可得

$$x \equiv D_1 a^2 + 1 \equiv \begin{cases} D_1 + 1 \pmod{8}, & \text{当 } a \text{ 为奇数时} \\ 1, 4D_1 + 1 \pmod{8}, & \text{当 } a \text{ 为偶数时} \end{cases}$$

当  $D_1 \equiv 5 \pmod{12}$  时,  $D_1 \equiv 1, 5 \pmod{8}$ ,

$$x \equiv \begin{cases} 2 \pmod{8}, & \text{当 } a \text{ 为奇数时} \\ 1, 5 \pmod{8}, & \text{当 } a \text{ 为偶数时} \end{cases}$$

此时有

$$x^2 + x + 1 \equiv 3 \pmod{8}$$

当  $D_1 \equiv 8 \pmod{12}$  时,  $D_1 \equiv 0, 4 \pmod{8}$ ,

$$x \equiv \begin{cases} 1, 5 \pmod{8}, & \text{当 } a \text{ 为奇数时} \\ 1 \pmod{8}, & \text{当 } a \text{ 为偶数时} \end{cases}$$

此时有

$$x^2 + x + 1 \equiv 3 \pmod{8}$$

由(15)式的后式得  $2 \nmid p b^2$ , 故  $2 \nmid b^2$ , 所以  $b^2 \equiv 1 \pmod{8}$ , 而  $p = 3(12r + 7)(12r + 8) + 1$ , 因此  $p \equiv 1, 5 \pmod{8}$ ,  $p b^2 \equiv 1, 5 \pmod{8}$ , 而  $x^2 + x + 1 \equiv p b^2 \pmod{8}$ , 所以情形(I)不成立。

情形(II), 由  $x - 1 = 3D_1 a^2$  和  $x^2 + x + 1 = 3p b^2$  可得

$$(2D_1 a^2 + 1)^2 + 1 = p(2b)^2 \quad (17)$$

从(17)式可知  $(X, Y) = (2b, 2D_1 a^2 + 1)$  是方程(13)的一组解。因为  $p = 3(12r + 7)(12r + 8) + 1$ , 所以方程(13)的最小正整数解是  $(X_1, Y_1) = (2, 24r + 15)$ 。根据文献[9]的结果可得

$$2b\sqrt{p} + (2D_1 a^2 + 1)\sqrt{3} = (2\sqrt{p} + (24r + 15)\sqrt{3})^t$$

其中,  $t$  是正奇数, 从而  $2D_1 a^2 + 1 \equiv 0 \pmod{(24r + 15)}$ , 即  $2D_1 a^2 + 1 \equiv 0 \pmod{3}, 4D_1^2 a^2 \equiv -2D_1 \pmod{3}$ , 因此  $\left(\frac{-2D_1}{3}\right) = 1$ , 其中  $\left(\frac{-2D_1}{3}\right)$  表示模的勒让德符号, 然而, 由  $D_1 \equiv 5, 8 \pmod{12}$  得  $D_1 \equiv 2 \pmod{3}$ , 故  $\left(\frac{-2D_1}{3}\right) = \left(\frac{-2}{3}\right)\left(\frac{D_1}{3}\right) = -1$  矛盾。故情形(II)不成立。

综上所述, 方程(3)在题设条件下无解。

### 参考文献:

[1] Mordell L J. Diophantine equation[M]. London America press 1969

[2] 柯召, 孙琦. 关于丢番图方程  $x^3 \pm 1 = Dy^2$  [J]. 中国科学, 1981, 24(12): 1453-1457.

[3] 段辉明. 关于不定方程  $x^3 - 1 = Dy^2$  [J]. 贵州师范大学学报: 自然科学版, 2005, 23(3): 67-69

[4] 彭成刚. 关于不定方程  $x^3 + 1 = 129y^2$  [J]. 四川理工学院学报: 自然科学版, 2009, 22(3): 6-7.

[5] 乐茂华. 关于 Diophantine 方程  $x^3 + 1 = py^2$  [J]. 广西师范学院学报: 自然科学版, 2005 22(4): 22-23

[6] 张淑静. 关于 Diophantine 方程  $x^3 \pm 1 = Dy^2$  [J]. 曲阜师范大学学报, 2009 35(4): 47-49

[7] 倪谷炎. 关于不定方程  $x^3 + 1 = Dy^2$  [J]. 哈尔滨师范大学: 自然科学学报, 1999, 15(3): 13-15

[8] 倪谷炎. 关于不定方程  $x^3 = Dy^2 + 1$  [J]. 国防科技大学学报, 1999, 2(5): 109-111.

[9] Walker D T. On the Diophantine equation  $mx^2 - ny^2 = \pm 1$  [J]. Amer Math Monthly, 1967, 74: 504-513

(下转第 523 页)

- [ J]. 大学数学, 2006, 22( 5): 102-106
- [ 6] V am a A K. A new proof of A. E. T in an' s approximation theorem [ J]. Journal of Approx Theory, 1976( 18): 57-62
- [ 7] 沈燮昌. 多项式插值 ( I ) — Lagrange 插值 [ J]. 数学进展, 1983, 12( 12): 193-214
- [ 8] 袁学刚, 何甲兴. 关于  $|$  类插值多项式的最高收敛阶 [ J]. 工程数学学报, 2001, 18( 3): 117-120
- [ 9] Yuan Xue gang W ei Ping. On two revised nodes of S. N. Bernstein interpolation process [ J]. Le Mat em atic he, 2001 ( 17): 39-48
- [ 10] 林鹭, 黄旭东. 拉格朗日插值多项式的  $|$  种并行算法 [ J]. 厦门大学学报: 自然科学版, 2004, 43( 5): 592-595
- [ 11] 盛中平, 王晓辉, 孙雪楠. 多点多重 N ew ton 型插值公式 [ J]. 东北师大学报: 自然科学版, 2007, 40( 2): 136-137

## Two Construction Methods of Interpolation Polynomial in Finite Field

YE Jun<sup>1,2</sup>, SU Yue-bin<sup>1</sup>

(1. School of Science, Sichuan University of Science & Engineering, Zigong 643000, China)

2. School of Mathematics and Computational Science, Guilin University of Electronic Technology, Guilin 541004, China)

**Abstract** Interpolation polynomials established in real number field may bring large error because of the accuracy limitations, rounding error and truncation error of computers. Problems of interpolation polynomials is considered in finite field in this paper; a theorem about the existence and uniqueness of interpolation polynomial in finite field is proposed, and then the theorem is proved strictly. Then two construction methods to gain the interpolation polynomials in finite field is also proposed by extending Lagrange interpolation and Newton interpolation to the finite field. At last, some examples are given to verify the correctness of the two methods.

**Key words** Lagrange interpolation polynomial, Newton interpolation polynomial, finite field, existence, uniqueness

(上接第 520 页)

## On the Diophantine Equation $x^3 \pm 1 = Dy^2$

LIANG Yong, HAN Yun-na

(Department of Mathematics, Northwest University, Xi'an 710127, China)

**Abstract** Using the properties of congruence, Legendre symbol and some other methods in number theory, the solutions of Diophantine equation  $x^3 \pm 1 = Dy^2$  are investigated, where  $D$  is square-free positive integer,  $D = D_1 p$ ,  $D_1$  cannot be divided by the prime number 3 or  $6k + 1$ , and  $p$  is an odd prime,  $p = 3(12r + 7)(12r + 8) + 1$ ,  $r$  is a positive integer. We prove that if  $D_1 \equiv 7 \pmod{12}$ , the equation  $x^3 + 1 = Dy^2$  has no positive integer solution, and if  $D_1 \equiv 5, 8 \pmod{12}$ , the  $x^3 - 1 = Dy^2$  has no positive integer solution.

**Key words** Diophantine equation, congruence, positive integer solution, Legendre symbol