

关于超椭圆方程 $x^p = 2y^2 + 3$ *

罗 明¹, 林丽娟²

(1. 重庆师范大学 数学科学学院, 重庆 401331; 2. 重庆化工职业学院 通识教育学院, 重庆 长寿 401228)

摘要: 设 p 为奇素数, 利用代数数论和初等数论相结合的方法证明了超椭圆方程 $x^p = 2y^2 + 3$ 无正整数解。

关键词: 不定方程; 超椭圆方程; 代数数

中图分类号: O156

文献标志码: A

文章编号: 1672-6693(2023)05-0096-03

设 p 是奇素数, 形如 $Ax^p = By^2 + C$ 的不定方程是一种重要的不定方程类型。当 $p > 3$ 时称为超椭圆方程, 有着较长的研究历史^[1-6], 但以往的研究都主要着重于情形 $B = 1$ 或 $C = 1$ 。本文研究不定方程 $x^p = 2y^2 + 3$, 对该方程没有正整数解进行证明。

令 α 是一个代数整数, $K = \mathbb{Q}(\alpha)$ 是一个代数数域, 即有理数域 $\mathbb{Q}$ 上的有限次代数扩域。 O_K 表示 K 中全部代数整数构成的环, 则 O_K 是一个整环; 但如果 O_K 不是主理想环, 则 O_K 不是唯一分解环。然而, 根据 Kummer 和 Dedekind 在代数数论领域的奠基性工作^[7], O_K 的每个非零理想(也习惯地称为 K 的理想)均可唯一地分解为有限个素理想的乘积, 这也是本文使用代数数论方法时的主要依据。

设 $A = [\alpha_1, \alpha_2, \dots, \alpha_m]$, $B = [\beta_1, \beta_2, \dots, \beta_n]$, 即 A, B 分别是由 $\alpha_1, \alpha_2, \dots, \alpha_m$ 和 $\beta_1, \beta_2, \dots, \beta_n$ 生成的理想, 则 $A|B \Leftrightarrow A \supseteq B \Leftrightarrow \beta_1, \beta_2, \dots, \beta_n \in A$ 。换言之, 对于 K 中 2 个理想, 整除即包含。此外, A, B 的最大公因子 $(A, B) = A + B = [\alpha_1, \alpha_2, \dots, \alpha_m, \beta_1, \beta_2, \dots, \beta_n]$, 乘积 $AB = [\alpha_1\beta_1, \alpha_2\beta_2, \dots, \alpha_m\beta_n]$ 。又设 K 的理想类数为 h , 熟知, 对于 K 的每一个理想 A , A^h 必为主理想。由此可以推出, 当 A^k 是主理想, 并且 $(h, k) = 1$ 时, A 一定也是主理想。更多的相关理论可查阅文献^[7-8]。

此外, 本文使用文献^[8]中记号 $\text{pot}_p a = n$ 表示 $p^n \parallel a$, 即 p^n 恰整除 a , 其中 p 是素数, a 是非零整数。以下性质显然成立: 1) $\text{pot}_p ab = \text{pot}_p a + \text{pot}_p b$; 2) $\text{pot}_p a^k = k \text{pot}_p a$ 。

下面给出本文的结论并证明。

定理 设 p 是奇素数, 不定方程 $x^p = 2y^2 + 3$ 无正整数解。

证明 原方程可化为 $4y^2 + 6 = 2x^p$, 在 $\mathbb{Q}(\sqrt{-6})$ 中分解为 $(2y + \sqrt{-6})(2y - \sqrt{-6}) = 2x^p$, 得理想等式:

$$[2y + \sqrt{-6}][2y - \sqrt{-6}] = [2][x]^p. \quad (1)$$

设最大公因理想 $D = ([2y + \sqrt{-6}], [2y - \sqrt{-6}]) = [2y + \sqrt{-6}, 2y - \sqrt{-6}]$, 则 $2\sqrt{-6} \in D, 12 \in D, 2x^p \in D$ 。由原方程知 $2 \nmid x, 3 \nmid x$, 所以 $(12, 2x^p) = 2 \in D$, 从而有 $\sqrt{-6} \in D$, 因此 $D|[2, \sqrt{-6}]$ 。显然有 $[2, \sqrt{-6}]|D$, 所以 $D = [2, \sqrt{-6}], D^2 = [4, 2\sqrt{-6}, -6] = [2]$ 。

由式(1)和理想的唯一分解性得: $[2y + \sqrt{-6}] = DA^p$, 其中 A 是 $\mathbb{Q}(\sqrt{-6})$ 中理想。

于是有 $D^{p-1}[2y + \sqrt{-6}] = D^p A^p = (DA)^p$, 即 $2^{\frac{p-1}{2}}[2y + \sqrt{-6}] = (DA)^p$ 。因为 $\mathbb{Q}(\sqrt{-6})$ 的类数为 2, p 是奇素数, $(2, p) = 1$ 。因此 DA 必为主理想, 又 $\mathbb{Q}(\sqrt{-6})$ 的单位仅有 ± 1 , 可得:

$$2^{\frac{p-1}{2}}(2y + \sqrt{-6}) = (a + b\sqrt{-6})^p, a, b \in \mathbb{Z}.$$

负号可纳入右端括号中。由此得:

* 收稿日期: 2022-10-01 修回日期: 2022-12-04 网络出版时间: 2023-06-25T10:53

资助项目: 重庆市教育委员会科学技术研究项目(No. KJQN202204501); 重庆化工职业学院校级科研课题(No. HZY2021-KJ03)

第一作者简介: 罗明, 男, 教授, 博士, 研究方向为数论, E-mail: luoming1958@126.com

网络出版地址: <https://link.cnki.net/urlid/50.1165.N.20230623.1019.002>

$$2^{\frac{p-1}{2}} \cdot 2y = \sum_{k=0}^{(p-1)/2} \binom{p}{2k} a^{p-2k} b^{2k} (-6)^k, \quad (2)$$

$$2^{\frac{p-1}{2}} = \sum_{k=0}^{(p-1)/2} \binom{p}{2k+1} a^{p-(2k+1)} b^{2k+1} (-6)^k. \quad (3)$$

由式(2)得 $2|a$, 因此式(3)两端可以消去 $2^{\frac{p-1}{2}}$, 得:

$$1 = \sum_{k=0}^{(p-1)/2} \binom{p}{2k+1} \left(\frac{a}{2}\right)^{p-(2k+1)} b^{2k+1} (-3)^k 2^{\frac{p-1}{2}-k}. \quad (4)$$

因此 $b \nmid 1$, 所以 $b = \pm 1$. 对式(4)取模 4 得:

$$p(p-1) \left(\frac{a}{2}\right)^2 b^{p-2} + b^p \equiv 1 \pmod{4}, \quad (5)$$

对式(4)取模 3, 得:

$$p \left(\frac{a}{2}\right)^{p-1} 2^{\frac{p-1}{2}} b \equiv 1 \pmod{3}. \quad (6)$$

下面分 2 种情况讨论。

情形 1, 当 $p \equiv 1 \pmod{4}$ 时, 由式(5)知 $b^p \equiv 1 \pmod{4}$, 所以 $b = 1$.

将 $b = 1$ 代入式(6)得 $p \left(\frac{a}{2}\right)^{p-1} 2^{\frac{p-1}{2}} \equiv 1 \pmod{3}$, 则 $p \equiv 1 \pmod{3}$, 即 $3 | (p-1)$, 且 $3 \nmid a$. 将 $b = 1$ 代入式(4)并变形得:

$$\begin{aligned} - \sum_{k=2}^{(p-1)/2} \binom{p}{2k+1} \left(\frac{a}{2}\right)^{p-(2k+1)} (-3)^k 2^{\frac{p-1}{2}-k} &= \binom{p}{1} \left(\frac{a}{2}\right)^{p-1} 2^{\frac{p-1}{2}} + \binom{p}{3} \left(\frac{a}{2}\right)^{p-3} (-3) 2^{\frac{p-3}{2}} - 1 = \\ &= (p-1) \left[\left(\frac{a}{2}\right)^{p-1} 2^{\frac{p-1}{2}} - p(p-2) \left(\frac{a}{2}\right)^{p-3} 2^{\frac{p-5}{2}} \right] + \left(\frac{a}{2}\right)^{p-1} 2^{\frac{p-1}{2}} - 1. \end{aligned} \quad (7)$$

由 $p \equiv 1 \pmod{3}$ 及 $p \equiv 1 \pmod{4}$ 知, 对于方括号中整数有:

$$\left(\frac{a}{2}\right)^{p-1} 2^{\frac{p-1}{2}} - p(p-2) \left(\frac{a}{2}\right)^{p-3} 2^{\frac{p-5}{2}} \equiv 1 - 2 \times 1 \times 1 \equiv 2 \pmod{3}.$$

即该整数不含素因数 3。

但是:

$$\begin{aligned} \text{pot}_3 \left(\left(\frac{a}{2}\right)^{p-1} 2^{\frac{p-1}{2}} - 1 \right) &= \text{pot}_3 \left(\left(\frac{a^2}{2}\right)^{\frac{p-1}{2}} - 1 \right) = \text{pot}_3 \left(\left(\frac{a^4}{4}\right)^{\frac{p-1}{4}} - 1 \right) = \\ &= \text{pot}_3 \left(\frac{a^4}{4} - 1 \right) + \text{pot}_3 \left(\frac{p-1}{4} \right) > \text{pot}_3(p-1). \end{aligned}$$

因此有 $\text{pot}_3 \left(\binom{p}{1} \left(\frac{a}{2}\right)^{p-1} 2^{\frac{p-1}{2}} + \binom{p}{3} \left(\frac{a}{2}\right)^{p-3} (-3) 2^{\frac{p-3}{2}} - 1 \right) = \text{pot}_3(p-1)$.

另一方面, 对式(7)求和项中各项有:

$$\begin{aligned} \text{pot}_3 \left(\binom{p}{2k+1} \left(\frac{a}{2}\right)^{p-(2k+1)} (-3)^k 2^{\frac{p-1}{2}-k} \right) &= \text{pot}_3 \left(\frac{p(p-1)}{(2k+1) \cdot 2k} \binom{p-2}{2k-1} \right) + k \geq \\ &= \text{pot}_3(p-1) + k - \text{pot}_3 r, r = 2k+1 \text{ 或 } 2k. \end{aligned}$$

由 $k \geq 2$ 可得 $3^k = (1+2)^k > 1+2k$, 所以 $3^k \nmid r$, $\text{pot}_3 r < k$.

因此有 $\text{pot}_3 \left(\sum_{k=2}^{(p-1)/2} \binom{p}{2k+1} \left(\frac{a}{2}\right)^{p-(2k+1)} (-3)^k 2^{\frac{p-1}{2}-k} \right) > \text{pot}_3(p-1)$, 则式(7)不能成立。

情形 2, 当 $p \equiv 3 \pmod{4}$ 时, 假如 $2 \mid \frac{a}{2}$, 对式(4)取模 8 得: $b^p (-3)^{\frac{p-1}{2}} \equiv 1 \pmod{8}$, 即 $\pm 5 \equiv 1 \pmod{8}$, 矛盾。

故 $2 \nmid \frac{a}{2}$, 又由式(5)得 $3b \equiv 1 \pmod{4}$, 故 $b = -1$. 将 $b = -1$ 代入式(6)得 $p \left(\frac{a}{2}\right)^{p-1} 2^{\frac{p-1}{2}} \equiv -1 \pmod{3}$, 从而 $p \equiv 1 \pmod{3}$, 即 $3 | p-1$, 且 $3 \nmid a$.

将 $b = -1$ 代入式(4)并变形得:

$$-\sum_{k=2}^{(p-1)/2} \binom{p}{2k+1} \left(\frac{a}{2}\right)^{p-(2k+1)} (-3)^k 2^{\frac{p-1}{2}-k} = \binom{p}{1} \left(\frac{a}{2}\right)^{p-1} 2^{\frac{p-1}{2}} + \binom{p}{3} \left(\frac{a}{2}\right)^{p-3} (-3) 2^{\frac{p-3}{2}} + 1 =$$

$$(p-1) \left[\left(\frac{a}{2}\right)^{p-1} 2^{\frac{p-1}{2}} - p(p-2) \left(\frac{a}{2}\right)^{p-3} 2^{\frac{p-5}{2}} \right] + \left(\frac{a}{2}\right)^{p-1} 2^{\frac{p-1}{2}} + 1. \quad (8)$$

其中: $\left(\frac{a}{2}\right)^{p-1} 2^{\frac{p-1}{2}} - p(p-2) \left(\frac{a}{2}\right)^{p-3} 2^{\frac{p-5}{2}} \equiv 2-1 \times 2 \times 2 \equiv 1 \pmod{3}$ 。

然而

$$\text{pot}_3 \left(\left(\frac{a}{2}\right)^{p-1} 2^{\frac{p-1}{2}} + 1 \right) = \text{pot}_3 \left(\left(\frac{a}{2}\right)^{p-1} 2^{\frac{p-1}{2}} + 1 \right) \left(\left(\frac{a}{2}\right)^{p-1} 2^{\frac{p-1}{2}} - 1 \right) = \text{pot}_3 \left(\left(\frac{a^2}{2}\right)^{2 \times \frac{p-1}{2}} - 1 \right) =$$

$$\text{pot}_3 \left(\left(\frac{a^2}{2}\right)^2 - 1 \right) + \text{pot}_3 \left(\frac{p-1}{2} \right) > \text{pot}_3(p-1)。$$

因此,式(8)最右端被 3 的 $\text{pot}_3(p-1)$ 次方恰好整除。

与情形 1 相同,可证明式(8)左端各项含因子 3 的个数大于 $\text{pot}_3(p-1)$ 。因此,式(8)不能成立。

综上所述,不定方程 $x^p = 2y^2 + 3$ 无正整数解。

证毕

参考文献:

- [1] 乐茂华. Gel'fond-Baker 方法在丢番图方程中的应用[M]. 北京:科学出版社,1998.
LE M H. The application of Gel'fond-Baker method in Diophantine equation[M]. Beijing: Science Press, 1998.
- [2] COHN J H E. The Diophantine equation $x^n = Dy^2 + 1$ [J]. Acta Arithmetica, 2003, 106: 73-83.
- [3] GODINHO H, NEUMANN V G L. The Diophantine equation $x^2 + p^a q^b = y^q$ [J]. International Journal of Number Theory, 2021, 17(9): 1-18.
- [4] KIHARA S. On coprime integral solutions of $y^2 = x^3 + k$ [J]. Proceedings of the Japan Academy, Ser A, 1987, 63: 13-16.
- [5] LE M H. On the Diophantine equation $2^n + px^2 = y^p$ [J]. Proceeding of the American Mathematical Society, 1995, 123(2): 321-326.
- [6] BAKER A. Bounds of the hyperelliptic equation [J]. Mathematical Proceeding of the Cambridge Philosophical Society, 1969, 65(2): 439-444.
- [7] 冯克勤. 代数数论[M]. 北京:科学出版社,2000.
FENG K Q. Algebraic number theory[M]. Beijing: Science Press, 2000.
- [8] 柯召,孙琦. 数论讲义(下册)[M]. 北京:高等教育出版社,1987.
KE Z, SUN Q. Lectures on number theory (volume 2)[M]. Beijing: Higher Education Press, 1987.

On the Hyperelliptic Equation $x^p = 2y^2 + 3$

LUO Ming¹, LIN Lijuan²

(1. School of Mathematical Sciences, Chongqing Normal University, Chongqing 401331;

2. Department of General Studies, Chongqing Chemical Industry Vocational College, Changshou Chongqing 401226, China)

Abstract: Let p be an odd prime, using methods of algebraic and elementary number theory, it proves that the Diophantine equation $x^p = 2y^2 + 3$ has no integer solution.

Keywords: diophantine equation; hyperelliptic equation; algebraic number theory

(责任编辑 黄 颖)