

关于一个不定方程组正整数解的上界

贺腊荣

(西北大学数学系, 西安 710127)

摘要:运用 Baker 方法得到不定方程组 $13x^2 - 11y^2 = 2$, $48x^2 - 13z^2 = 35$ 正整数解的上界, 即记 $S = \{(x, y, z) \mid x, y, z \in \mathbb{Z} \text{ 并且满足方程组 } 13x^2 - 11y^2 = 2, 48x^2 - 13z^2 = 35\}$, $T = \{y \mid (x, y, z) \in S\}$ 若能求得 T 的上界, 只要将解内的 y 值代入方程组, 就可求得方程组的全部正整数解。可以得到上界方程组 $13x^2 - 11y^2 = 2$, $48x^2 - 13z^2 = 35$ 的上界为 $(x, y, z) = (0.92 \times 24^{18^{93}}, 24^{18^{93}}, 1.92 \times 24^{18^{93}})$ 。

关键词:不定方程组; 解的上界; Baker 方法

中图分类号: O156

文献标识码: A

引言

在不定方程组的研究中, 整数解绝对值的上界的确定是个重要的问题, 因为一旦知道这一上界, 只要把界内的整数代入原方程(组), 即可得到全部解。目前对于不定方程

$$\begin{cases} a_2x^2 - a_1y^2 = a_2 - a_1 \\ a_3y^2 - a_2z^2 = a_3 - a_2 \end{cases} \quad (1)$$

(a_1, a_2, a_3 为正整数且其中任两个数之积与 1 的和为平方数) 的整数解的上界已有不少学者进行了研究, 如陈志云^[1]于 1997 年解决了当 $a_1 = 7, a_2 = 9, a_3 = 32$ 时方程组 (1) 的解的上界, 2006 年, 李杨^[2]解决了 $a_1 = 5, a_2 = 7, a_3 = 24$ 时方程组 (1) 的解的上界, 胡青龙等^[3], 郑兆顺^[4]分别于 2006 年, 2008 年解决了 $a_1 = 3, a_2 = 5, a_3 = 16$ 与 $a_1 = 9, a_2 = 11, a_3 = 40$ 时方程组 (1) 的解的上界, 本文运用 Baker 方法研究当 $a_1 = 11, a_2 = 13, a_3 = 48$ 时, 即不定方程

$$\begin{cases} 13x^2 - 11y^2 = 2 \\ 48y^2 - 13z^2 = 35 \end{cases} \quad (2)$$

的解的上界。

方程组 (2) 可化为

$$\begin{cases} 169x^2 - 143y^2 = 26 \\ 624y^2 - 169z^2 = 455 \end{cases} \quad (3)$$

令 $13x = x', y = y', 13z = z'$, 方程组 (3) 变为

$$\begin{cases} x'^2 - 143y^2 = 26 \\ z'^2 - 624y^2 = -455 \end{cases}$$

即

$$\begin{cases} x^2 - 143y^2 = 26 \\ z^2 - 624y^2 = -455 \end{cases}$$

由文献 [5-6] 易知 Pell 方程 $x^2 - 143y^2 = 1$ 的基本解为 $12 + \sqrt{143}$ 不定方程 $x^2 - 143y^2 = 26$ 的基本解为 $13 + \sqrt{143}$, 所以方程 $x^2 - 143y^2 = 26$ 的所有正整数解为

$$\begin{cases} x_m + y_m \sqrt{143} = (13 + \sqrt{143})(12 + \sqrt{143})^m \\ m \geq 0 \end{cases} \quad (4)$$

又因为

$$x_{m+1} + y_{m+1} \sqrt{143} = (x_m + y_m \sqrt{143})(12 + \sqrt{143})$$

所以有

$$\begin{cases} x_{m+1} = 12x_m + 143y_m \\ y_{m+1} = x_m + 12y_m \\ m = 0, 1, 2, \dots, x_0 = 13, y_0 = 1 \end{cases} \quad (5)$$

不难得出 Pell 方程 $z^2 - 624y^2 = 1$ 的基本解为 $25 + \sqrt{624}$ 不定方程 $z^2 - 624y^2 = -455$ 的基本解为 $13 +$

$\sqrt{624}$ 或 $-13 + \sqrt{624}$ 所以 $z^2 - 624y^2 = -455$ 的所有正整数解为

$$\begin{cases} z_n + y_n \sqrt{624} = (13 + \sqrt{624})(25 + \sqrt{624})^n \\ n = 0, 1, 2, \dots \end{cases} \quad (6)$$

或

$$\begin{cases} z_n + y_n \sqrt{624} = (-13 + \sqrt{624})(25 + \sqrt{624})^n \\ n = 0, 1, 2, \dots \end{cases} \quad (7)$$

由 (4) 式, 得

$$\begin{cases} x_m - y_m \sqrt{143} = (13 - \sqrt{143})(12 - \sqrt{143})^m \\ m \geq 0 \end{cases} \quad (8)$$

由 (4) 式与 (8) 式得

$$2\sqrt{143}y_m = (13 + \sqrt{143})(12 - \sqrt{143})^m - (13 - \sqrt{143})(12 + \sqrt{143})^m$$

类似有

$$2\sqrt{624}y_n = (13 + \sqrt{624})(25 + \sqrt{624})^n - (13 - \sqrt{624})(25 - \sqrt{624})^n$$

$$2\sqrt{624}y_n = (-13 + \sqrt{624})(25 + \sqrt{624})^n + (13 + \sqrt{624})(25 - \sqrt{624})^n$$

令 $y_m = y_n$ 得

$$\frac{(13 + \sqrt{143})(12 + \sqrt{143})^m}{\sqrt{143}} + \frac{(\sqrt{143} - 13)(12 + \sqrt{143})^{-m}}{\sqrt{143}} = \frac{(13 + \sqrt{624})(25 + \sqrt{624})^n}{\sqrt{624}} + \frac{(\sqrt{624} - 13)(25 + \sqrt{624})^{-n}}{\sqrt{624}} \quad (9)$$

$$\frac{(13 + \sqrt{143})(12 + \sqrt{143})^m}{\sqrt{143}} + \frac{(\sqrt{143} - 13)(12 + \sqrt{143})^{-m}}{\sqrt{143}} = \frac{(-13 + \sqrt{624})(25 + \sqrt{624})^n}{\sqrt{624}} + \frac{(\sqrt{624} + 13)(25 + \sqrt{624})^{-n}}{\sqrt{624}} \quad (10)$$

若 $(x, y, z) \in S$, 则必存在 m, n , 使得 $y = y_n = y_m$, 从而使 (9) 式或 (10) 式成立. 因此, 如果求得 (9) 式或 (10) 式成立的 m 的上界, 就可以通过 (5) 式求得 y_m 的上界, 从而得 T 的上界.

1 主要引理及定理

引理 1^[7] 设 $\alpha_1, \alpha_2, \dots, \alpha_k$ 是 $k(k \geq 2)$ 非零代数, $\alpha_i (i = 1, 2, \dots, k)$ 的次数和高分别不超过 $d(d \geq 4)$ 和 $A(A \geq 4)$. 若存在整数 b_1, b_2, \dots, b_k 满足 $0 < b_1 \lg \alpha_1 +$

$b_2 \lg \alpha_2 + \dots + b_k \lg \alpha_k < e^{-\delta H}$, 其中 $0 < \delta \leq 1, H = \max(|b_1|, |b_2|, \dots, |b_k|)$, 则 $H < (4^k \delta^{-1} d^{2k} \lg A)^{(2k+1)^2}$. 这里 α 的次数不妨设为 n , 是指 α 满足一个 n 次整系数代数方程, 而不满足任何低于 n 次的整系数代数方程; α 高不妨设为 h , 是指 α 所适合的整系数不可约多项式 $a_m x_m + \dots + a_1 x_1 + a_0$ 的系数 $a_j (j = 0, 1, \dots, m)$ 绝对值的最大值, 即 $h = \max(|a_m|, \dots, |a_0|)$.

这个结论是由 Baker A 证明的^[7], 他还运用此结论给出了某些类型的不定方程整数解绝对值的上界, 按照 Baker A 的这种思路来研究不定方程 (组) 的方法, 通常称为 Baker A 方法.

定理 1 (1) 若 (9) 式成立, 则 $m = n = 0$ 或 $m > n$ (2) 若 (10) 式成立, 则 $m = n = 2$ 或 $m > n$.

定理 2 (1) 若 (9) 式成立, 且 $m \geq 3$ 则 $\lg \frac{P}{Q} < 0.91099P^{-2}$; (2) 若 (10) 式成立, 且 $m \geq 3$ 则 $\lg \frac{P}{Q_1} < 0.91099P^{-2}$, 这里 $Q_1 = \frac{(-13 + \sqrt{624})(25 + \sqrt{624})^n}{\sqrt{624}}$.

定理 3 (1) 若 (9) 式成立, 则 $0 \leq m \leq 18^{393}$, (2) 若 (10) 式成立, 则 $2 \leq m \leq 18^{393}$.

定理 4 不定方程 (2) 的正整数解得上界为 $(x, y, z) = (0.92 \times 24^{18^{393}}, 24^{18^{393}}, 1.92 \times 24^{18^{393}})$.

2 定理证明

定理 1 证明 由 (4) 式知, 当 $m = 0, y_m = 1$ 若 (9) 式成立, 则必有 $y_n = 1$. 由 (6) 式得当 $n = 0$ 时, $y_n = 1$ 且 y_n 随 n 的增大而增大, 故只可能是 $n = 0$.

当 $m > 0$ 时, 由 (5) 式知 $y_m > 1$, 此时, 若 (9) 式成立, 则必有 $y_n > 1$, 由此得 $n > 0$ 记

$$P = \frac{(13 + \sqrt{143})(12 + \sqrt{143})^m}{\sqrt{143}} \quad Q = \frac{(13 + \sqrt{624})(25 + \sqrt{624})^n}{\sqrt{624}} \quad (11)$$

则 $P > 2, Q > 1$ 且由 (9) 式得

$$P - \frac{2}{11}P^{-1} = Q + \frac{35}{48}Q^{-1}$$

则 $P - Q = \frac{2}{11}P^{-1} + \frac{35}{48}Q^{-1} > 0$ 故 $P > Q$, 再利用 (11) 式得

$$\frac{(13 + \sqrt{143})(12 + \sqrt{143})}{\sqrt{143}} >$$

$$\frac{(13 + \sqrt{624})(25 + \sqrt{624})^n}{\sqrt{624}}$$

故

$$(12 + \sqrt{143})^m > \frac{\sqrt{143}(13 + \sqrt{624})}{\sqrt{624}(13 + \sqrt{143})} (25 + \sqrt{624})^n$$

从而 $m \ln(12 + \sqrt{143}) > \ln 0.73 + \ln(25 + \sqrt{624})^n$, 所以 $3.176m > -0.315 + 0.3.912n$, 即 $3.176(m - n) > 0.736n - 0.315 \geq 0.412 > 0$ 即 $n > 0, n \in \mathbf{Z}$ 所以 $m > n$ 定理 1(1)得证. 定理 1(2)的证明与定理 1(1)类似.

定理 2证明 若(9)式成立, 且 $m \geq 3$ 由定理 1可知 $n \geq 1$, 于是由(11)式可知 $P > 28702, Q > 76$ 从而 $\frac{1}{P} < \frac{1}{28702}, \frac{1}{Q} < \frac{1}{76}$ 则

$$Q = P - \frac{2}{11}P^{-1} - \frac{35}{48}Q^{-1} >$$

$$P - \frac{2}{11 \times 28702} - \frac{35}{48 \times 76} > P - \frac{1}{104}$$

故 $Q^{-1} < \frac{104}{104P - 1}$ 所以

$$P - Q = \frac{2}{11}P^{-1} + \frac{35}{48}Q^{-1} < \frac{2}{11}P^{-1} + \frac{35 \times 104}{48(104P - 1)}$$

又 $P > 28702$ 则

$$P - Q < \frac{2}{11}P^{-1} + \frac{35 \times 104}{104 - \frac{1}{28702}}P^{-1} = 0.91098510P^{-1}$$

于是 $0 < \frac{P-Q}{P} < 0.91098510P^{-2} < 1$, 当 $0 < x < 1$ 时,

$-(\lg(1-x)) < x + x^2$, 得

$$0 < \lg \frac{P}{Q} = -\lg(1 - \frac{P-Q}{P}) < -\lg(1 - 0.91098510P^{-2}) <$$

$$0.9109851P^{-2} + (0.9109851P^{-2})^2 < 0.91099P^{-2}$$

即证明了定理 2(1), 定理 2(2)的证明与定理 2(1)类似.

定理 3证明 由于

$$P > Q, \frac{P}{Q} = \frac{\sqrt{624}(13 + \sqrt{143})(12 + \sqrt{143})^m}{\sqrt{143}(13 + \sqrt{624})(25 + \sqrt{624})^n}$$

若(9)式成立, 且 $m \geq 3$ 由定理 2知

$$0 < \lg \frac{P}{Q} = M \lg(12 + \sqrt{143}) - n \lg(13 + \sqrt{624}) +$$

$$\lg \frac{\sqrt{624}(13 + \sqrt{143})}{\sqrt{143}(13 + \sqrt{624})} < 0.91099P^{-2} =$$

$$0.91099 \left[\frac{\sqrt{143}}{13 + \sqrt{143}} \right]^2 \times \frac{1}{(12 + \sqrt{143})^{2m}} <$$

$$0.209132 \times \frac{1}{(12 + \sqrt{143})^m} < e^{-m}$$

记

$$a_1 = 12 + \sqrt{143}, a_2 = 25 + \sqrt{624}$$

$$a_3 = \frac{\sqrt{624}(13 + \sqrt{143})}{\sqrt{143}(13 + \sqrt{624})}$$

$$a'_3 = \frac{\sqrt{624}(-13 + \sqrt{143})}{\sqrt{143}(\sqrt{624} + 13)}$$

则 a_1, a_2 分别满足 $x^2 - 24x + 1 = 0, x^2 - 50x + 1 = 0$ 且 $x^2 - 24x + 1, x^2 - 50x + 1$ 均为整系数不可约多项式. a_3 在四次域上的 3 个共轭根为:

$$a'_3 = \frac{\sqrt{624}(13 - \sqrt{624})}{-\sqrt{143}(13 + \sqrt{624})}$$

$$a''_3 = \frac{-\sqrt{624}(13 + \sqrt{143})}{\sqrt{143}(13 - \sqrt{624})}$$

$$a'''_3 = \frac{\sqrt{624}(13 - \sqrt{143})}{\sqrt{143}(13 - \sqrt{624})}$$

以这四个代数数为解的方程为:

$$(143 \times 455)^2 x^4 - 23223520320x^3 + 19543949568x^2 + 5790799872x + 624 \times 26^2 = 0$$

且方程左边为一整系数不可约多项式, 然后用引理 1 这里 $K = 3d = 4l = 23223520320, H = \max(m, n, 1) = m$, 所以

$$m < (4^3 \times 1 \times 4^{2 \times 3} \lg 23223520320)^{(2 \times 3 + 1)^2} = (4^{15} \times 10.4)^{49} < 18^{393}$$

又由于当 $m = n = 0$ 时(9)式成立, 即证明了定理 3(1).

仿照上面的证明过程, 将 Q 换成 Q' , 再应用引理 1 时将 a_3 换成 a'_3 , 即可证明定理 3(1)成立.

定理 4证明 由 $m < 18^{393}$ 和等式

$$2\sqrt{143}y_m = (13 + \sqrt{143})(12 - \sqrt{143})^m - (13 - \sqrt{143})(12 + \sqrt{143})^m, (m \geq 0)$$

可得, $y < 24^{18^{393}}$, 即 y 的上界为 $24^{18^{393}}$, 则不定方程组(2)可以求得正整数解, 为

$$(x, y, z) = (0.92 \times 24^{18^{393}}, 24^{18^{393}}, 1.92 \times 24^{18^{393}})$$

参考文献:

[1] 陈志云. 关于不定方程组 $x^2 - 7y^2 = 2, z^2 - 32y^2 = -23$ 的正整数解的上界[J]. 华中师范大学学报:自然科学版, 1997, 31(3): 253-256
 [2] 李杨. 关于不定方程组 $7x^2 - 5y^2 = 2, 24y^2 - 7z^2 = 17$ 正整数解的上界[J]. 重庆师范大学学报:自然科学版, 2006, 23(3): 33-35
 [3] 胡青龙, 李杨. 关于不定方程组正整数解的上界[J]. 重庆工商大学学报:自然科学版, 2006, 23(4): 45-47

- [4] 郑兆顺. 不定方程组 $11x^2 - 9y^2 = 2$, $40y^2 - 11z^2 = a_2z^2 = a_3 - a_2$ [J]. 四川大学学报: 自然科学版, 1992, 29(3): 348-351.
- [5] 柯召, 孙琦. 谈谈不定方程 [M]. 上海: 上海教育出版社, 1980.
- [6] 郑德勋. 关于不定方程 $a_2x^2 - a_1y^2 = a_2 - a_1$, $a_3y^2 - a_2z^2 = a_3 - a_2$ [J]. 四川大学学报: 自然科学版, 1992, 29(3): 348-351.
- [7] Baker A, Davnpirt H. The Equations $3x^2 - 2 = y^2$, $8x^2 - 7 = z^2$ [J]. Quart JM ath Oxford, 1969, 20(2): 129-137.

On the Upper Bound for the Positive Integer Solutions of the System of Diophantine Equations

HE La-rong

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

Abstract By Baker's method, this paper solves the upper bound for the positive integer solution of the system of Diophantine equations $\begin{cases} 13x^2 - 11y^2 = 2 \\ 48y^2 - 13z^2 = 35 \end{cases}$ was solved and let $S = \{ (x, y, z) \mid x, y, z \in \mathbb{Z}, \text{ and } 13x^2 - 11y^2 = 2, 48y^2 - 13z^2 = 35 \}$, $T = \{ y \mid (x, y, z) \in S \}$. If we can get the upper bounds of T and as long as we let y of solution put the system of Diophantine equations we may get all integer solutions of the system of Diophantine equations and we can get the upper bounds are $(x, y, z) = (0.92 \times 24^{18^{30}}, 24^{18^{30}}, 1.92 \times 24^{18^{30}})$.

Key words Diophantine equations system; the upper bound of solution; Baker's method

(上接第 33 页)

- [5] 刘太琳, 温巧燕, 刘子辉. 非二元量子循环码的一种图论方法构造 [J]. 中国科学, 2005, 30(6): 588-596.
- [6] 李卓, 邢莉娟, 王新梅. 一类量子循环码的构造方法 [J]. 西安电子科技大学学报: 自然科学版, 2007, 34(2): 187-189.
- [7] 蔡乐才. 量子纠错码的研究 [J]. 四川理工学院学报: 自然科学版, 2004, 17(4): 163-168.

Description of Stabilizer to Non-trivial Vector Space

CHENG Qian¹, YU Hu²

(1. School of Mathematics, Qinghai Normal University, Xining 810008, China

2. School of Mathematics, Dalian Jiaotong University, Dalian 116028, China)

Abstract All stabilizers of non-trivial vector space V_S is described as the subgroups of Pauli group G_1 by the necessary and sufficient condition that the subgroups of Pauli group become stabilizers and the operator property of the generating elements of stabilizers is discussed.

Key words Pauli group; stabilizer; generating element