关于单 K_4-群中的一个丢番图方程及其推广

何宗友

（宁波新芝生物科技股份有限公司, 浙江 宁波 315013）

摘要: 设 N 和 P 分别表示整数的集合和素数的集合, $d \in N, d > 0$ 且不是平方数, $p, q_i \in P, p > 3, q_i > 3, n_0, n_i, i, r \in N, n_0 \geqslant 1, n_i \geqslant 1, 1 \leqslant i \leqslant r$, 利用 Bilu、Hanrot 和 Voutier 关于 Lucas 数本原素因子存在性的结果研究了丢番图方程 $(p^m)^2 - d(2^{n_0} q_1^{n_1} q_2^{n_2} \cdots q_r^{n_r})^2 = 1$ 的解 $(p, q_1, q_2, \cdots, q_r, m, n_0, n_1, n_2, \cdots, n_r)$, 从而部分地解决了单 K_4-群中一个丢番图方程的求解问题.

关键词: 丢番图方程; Pell 方程; 解; Lucas 数列; 本原素因子

中图分类号: O156.7 **文献标识码:** A **文章编号:** 1001-5132（2012）02-0076-03

设 N 和 P 分别表示整数的集合和素数的集合, 1991 年, 施武杰[1]在研究单 K_4 -群的精细刻划时提出的一个问题, 即丢番图方程:

$$p^{2m} - 1 = 2^a 3^b q^n, p, q \in P, p > 3, q > 3, a, b, m, n \in N, a \geqslant 1, b \geqslant 1, m \geqslant 1, n \geqslant 1, \quad (1)$$

有哪些解 (p, q, a, b, m, n) ？从 Estes D、Guralnick R、Schacher M 和 Straus E 的结果可知, 丢番图方程(1)仅有限多组解满足 $n > 1$[2]; 1996 年, 乐茂华和徐广善[3]证明了: 丢番图方程(1)仅有两组解 $(p, q, a, b, m, n) = (577, 17, 7, 2, 1, 2), (97, 7, 6, 1, 1, 2)$; 2000 年, 袁平之[4]指出文献[3]的证明是错误的, 所以这个问题仍然是一个未解决的问题. 设 $d \in N, d > 0$ 且不是平方数, 笔者利用 Bilu、Hanrot 和 Voutier[5]关于 Lucas 数本原素因子存在性的结果研究了丢番图方程:

$$(p^m)^2 - d(2^{n_0} q_1^{n_1} q_2^{n_2} \cdots q_r^{n_r})^2 = 1, p, q_i \in P, p > 3, q_i > 3, n_0, n_i, i, r \in N, n_0 \geqslant 1, n_i \geqslant 1, 1 \leqslant i \leqslant r, \quad (2)$$

的解 $(p, q_1, q_2, \cdots q_r, m, n_0, n_1, n_2, \cdots n_r)$, 由此找到了丢番图方程(1)满足 $2 \mid n$ 的全部解 (p, q, a, b, m, n), 从而部分地回答了施武杰提出的问题.

定理 1 设 $x_n + y_n\sqrt{d} = \varepsilon^n$, $2^s \parallel x_1 y_1, \omega(d, h) = \omega(x_{2^{h-1}} x_{2^{h-2}} \cdots x_{2^1})$, $\omega_0 = \omega(x_1 y_1 / 2^s), n, s, h \in N$, $n \geqslant 1$, $s \geqslant 0, h \geqslant 1$, 这里, $\varepsilon = x_1 + y_1\sqrt{d}$ 是 Pell 方程 $x^2 - dy^2 = 1$ 的基本解, $\omega(n)$ 表示正整数 n 不同素因子的个数, 则当且仅当(i) $\omega(d, h) + \omega_0 = r, 2 \leqslant h \leqslant r + 1 - \omega_0$; (ii) $p'^{m'} = x_{2^h}, q_1'^{n_1'} q_2'^{n_2'} \cdots q_r'^{n_r'} = x_{2^{h-1}} x_{2^{h-2}} \cdots x_{2^1} \cdot (x_1 y_1 / 2^s)$ 时, 丢番图方程(2)仅有一组解; (iii) $(p, q_1, q_2, \cdots, q_r, m, n_0, n_1, n_2, \cdots, n_r) = (p', q_1', q_2', \cdots, q_r', m', h + s, n_1', n_2', \cdots, n_r')$.

定理 1 设 $2^s \parallel x_1 y_1, \omega(d, h) = \omega(x_{2^{h-1}} x_{2^{h-2}} \cdots x_{2^1}), \omega_0 = \omega(x_1 y_1 / 2^s), s, h \in N, s \geqslant 0, h \geqslant 1$, 其中, $\omega(n)$ 表示正整数 n 的不同素因子的个数, 则当且仅当(i) $\omega(d, h) + \omega_0 = r, 2 \leqslant h \leqslant r + 1 - \omega_0$; (ii) $p'^{m'} = x_{2^h}$, $q_1'^{n_1'} q_2'^{n_2'} \cdots q_r'^{n_r'} = x_{2^{h-1}} x_{2^{h-2}} \cdots x_{2^1} \cdot (x_1 y_1 / 2^s)$ 时, 丢番图方程(2)仅有一组解; (iii) $(p, q_1, q_2, \cdots q_r, m, n_0, n_1, n_2, \cdots, n_r) = (p', q_1', q_2', \cdots q_r', m', h + s, n_1', n_2', \cdots, n_r')$.

定理 2 丢番图方程(1)仅有两组解 $(p, q, a, b, m, n) = (577, 17, 7, 2, 1, 2), (97, 7, 6, 1, 1, 2)$ 满足 $2 \mid n$.

1 预备工作

首介绍一下 Bilu、Hanrot 和 Voutier[5]关于 Lucas 数本原素因子存在性的结果.

定义 1 设 α, β 为代数整数, $\alpha + \beta$ 和 $\alpha\beta$ 是非零互素的有理整数, 且 α / β 不是单位根, 则称 (α, β) 为 Lucas 数偶. 对于给定的 Lucas 数偶 (α, β), 定义 Lucas 数列为:

$$u_n(\alpha, \beta) = (\alpha^n - \beta^n) / (\alpha - \beta), n \in N^+,$$

收稿日期: 2011−06−30. 宁波大学学报（理工版）网址: http://3xb.nbu.edu.cn
作者简介: 何宗友（1972−）, 男, 陕西汉中人, 技术员, 主要研究方向: 数论. E-mail: hezongyou@126.com

两对 Lucas 数偶 (α_1,β_1) 和 (α_2,β_2) 称为等价的, 如果 $\alpha_1/\alpha_2=\beta_1/\beta_2=\pm1$.

定义 2　设 (α,β) 为 Lucas 数偶, 如果 $p\mid u_n(\alpha,\beta)$ 且 $p\nmid(\alpha-\beta)^2u_1(\alpha,\beta)\cdots u_{n-1}(\alpha,\beta)$, 则称 p 是 $u_n(\alpha,\beta)$ 的本原素因子. 对于两对等价的 Lucas 数偶 (α_1,β_1) 和 (α_2,β_2), 我们有 $u(\alpha_1,\beta_1)=\pm u(\alpha_2,\beta_2)$, 因此, 它们同时具有或不具有本原素因子.

BHV 定理[5]　对于任意大于 30 的整数 n, Lucas 数列第 n 项 $u_n(\alpha,\beta)$ 有本原素因子. 当 $n\leqslant30$ 时, 使 $u_n(\alpha,\beta)$ 没有本原素因子的 (α,β) 可以完全决定.

引理[5]　设 $5\leqslant n\leqslant30$, 且 $n\neq6$, 则所有使 $u_n(\alpha,\beta)$ 不具有本原素因子的 Lucas 数偶 (α,β) 可表示为 $(\alpha,\beta)=((a-\sqrt{b})/2,(a+\sqrt{b})/2)$ 及与它们等价的 Lucas 数偶, 其中 n,a,b 满足如下条件:

(1)　$n=5$ 时, $(a,b)=(1,5),(1,-7),(2,-40),(1,-11),(1,-15),(12,-76)$ 或 $(12,-1364)$;

(2)　$n=7$ 时, $(a,b)=(1,-7)$ 或 $(1,-19)$;

(3)　$n=8$ 时, $(a,b)=(1,-7)$ 或 $(2,-24)$;

(4)　$n=10$ 时, $(a,b)=(2,8),(5,-3)$ 或 $(5,-47)$;

(5)　$n=12$ 时, $(a,b)=(1,-5),(1,-7),(1,-11),(2,-56),(1,-15)$ 或 $(1,-19)$;

(6)　$n=13,18$ 或 30 时, $(a,b)=(1,-7)$.

2　定理的证明

2.1　定理 1 的证明

由 Pell 方程的解法得丢番图方程(2)的全部解 $(p,q_1,q_2,\cdots q_r,\ m,n_0,n_1,n_2,\cdots n_r)$ 由下式给出[6]:

$$p^m+2^{n_0}q_1^{n_1}q_2^{n_2}\cdots q_r^{n_r}\sqrt{d}=x_n+y_n\sqrt{d}=\varepsilon^n,\quad n\in N,n>0. \tag{3}$$

可设 $n=2^hl,h,l\in N,2\nmid l,h\geqslant0,l\geqslant1$, 由定义 1 可以验证 $(\alpha,\beta)=(x_1+y_1\sqrt{D},x_1-y_1\sqrt{D})$ 为 Lucas 数偶, 由(3)式及定义 1 可得 $y_{2n}=y_1u_{2n}(\alpha,\beta)$, 以及 $y_{2n}=2x_ny_n=2x_ny_1u_n(\alpha,\beta)$, 又由(3)式知 $x_n=p^m$, 因此,

$$u_{2n}(\alpha,\beta)=2p^mu_n(\alpha,\beta). \tag{4}$$

由(4)式及定义 2 知, 2 和 $u_n(\alpha,\beta)$ 的素因子都不是 $u_{2n}(\alpha,\beta)$ 的本原素因子, 因此如果 $u_{2n}(\alpha,\beta)$ 有本原素因子, 则只能是 p. 又由定义 1 可得:

$$u_{2^{h+1}}(\alpha,\beta)=2x_{2^h}u_{2^{h+1}}(\alpha,\beta). \tag{5}$$

另一方面, 由 $2\nmid l$ 及(3)式可知, $x_{2^h}\mid x_n$ 即 $x_{2^h}\mid p^m$, 注意到由 $x_{2^h}>1$ 得 $p\mid x_{2^h}$, 故由(5)式得 $p\mid u_{2^{h+1}}(\alpha,\beta)$, 如果 $l>1$, 则由 $n=2^hl$ 知, $2n>2^{h+1}$, 故由定义 2 知, p 不是 $u_{2n}(\alpha,\beta)$ 的本原素因子, 所以 $u_{2n}(\alpha,\beta)$ 没有本原素因子.

由 BHV 定理和引理排除 $2n=5$ 及 $2n\geqslant7$, 注意到 $l>1$ 且 $n=2^hl,2\nmid l,h\geqslant0$ 可得, 仅剩下 $n=3$, 因此, $p^m=x_3=x_1(4x_1^2-3)$, 注意到 $x_1>1$ 及 $\gcd(x_1,4x_1^2-3)=1$ 或 3, 因此仅有三种可能: (i) $x_1=p^m$, $4x_1^2-3=1$, 或(ii) $x_1=3,4x_1^2-3=3^{m-1}$, 或(iii) $x_1=3^{m-1},4x_1^2-3=3$. 由(i)可知, $x_1=1$, 从而 $y_1=0$ 不是正整数; 由(ii)可知, $33=3^{m-1}$ 不可能; 由(iii)可知, $2x_1^2=3$ 不可能. 这就证明了 $l=1$, 因此 $n=2^h$, $h\in N,h\geqslant0$. 代入(3)式可得:

$$p^m+2^{n_0}q_1^{n_1}q_2^{n_2}\cdots q_r^{n_r}\sqrt{d}=\varepsilon^{2^h},h\in N,h\geqslant0,$$

由 $2^s\parallel x_1y_1$ 及上式可得:

$$p^m=x_{2^h},2^{n_0}q_1^{n_1}q_2^{n_2}\cdots q_r^{n_r}=2^{h+s}x_{2^{h-1}}x_{2^{h-2}}\cdots x_{2^1}\cdot(x_1y_1/2^s). \tag{6}$$

由 $\gcd(x_{2^i},y_1)=\gcd(x_{2^i},x_{2^j})=1,0\leqslant i\neq j\leqslant h-1$ 得 $\gcd(x_{2^{h-1}},x_{2^{h-2}}x_{2^{h-3}}\cdots x_{2^1}\cdot(x_1y_1/2^s))=1$, 故 $\omega(d,h)>\omega(d,h-1)>\cdots>\omega(d,2)$, 即最多只有 1 个 h 满足(i), 由此及(6)式可得, 当且仅当(i)和(ii)成立时, 丢番图方程(2)只有一组解(iii). 定理 1 证完.

2.2　定理 2 的证明

设 (p,q,a,b,m,n) 是丢番图方程(1)满足 $2\mid n$ 的一组解, 只需研究 $2\nmid a,2\mid b$; $2\mid a,2\nmid b$及$2\nmid a,2\nmid b$ 三种情形.

按这三种情形,丢番图方程(1)分别写成:

$$(p^m)^2-2(2^{\frac{a-1}{2}}\cdot3^{\frac{b}{2}}\cdot q^{\frac{n}{2}})^2=1,2\nmid a,2\mid b, \tag{7}$$

$$(p^m)^2-3(2^{\frac{a}{2}}\cdot3^{\frac{b-1}{2}}\cdot q^{\frac{n}{2}})^2=1,2\mid a,2\nmid b, \tag{8}$$

$$(p^m)^2-6(2^{\frac{a-1}{2}}\cdot3^{\frac{b-1}{2}}\cdot q^{\frac{n}{2}})^2=1,2\nmid a,2\nmid b, \tag{9}$$

由(7)式可得, $d=2,r=2,(x_1,y_1)=(3,2),s=1,\omega_0=1,h=2,\omega(2,2)=1,\omega(2,2)+\omega_0=r,\omega(2,2)$ 满足定理 1 中的(i)式, $577^1=x_{2^2},3^{\frac{b}{2}}q^{\frac{n}{2}}=x_{2^1}\cdot(x_1y_1/2^s)=17\cdot3$ 满足定理 1 中的(ii)式, 故方程(7)仅有一组解 $(p,q,a,b,m,n)=(577,17,7,2,1,2)$.

当 $b>1$ 时, 由(8)式可得 $d=3,r=2,(x_1,y_1)=(2,1),s=1,\omega_0=0,2\leqslant h\leqslant3,\omega(3,2)=1,\omega(3,3)=2,\omega(3,3)+\omega_0=r$, $\omega(3,3)$ 满足定理 1 中的(i)式, $3^{\frac{b-1}{2}}q^{\frac{n}{2}}=x_{2^2}x_{2^1}\cdot(x_1y_1/2^s)=97\cdot7$ 不满足定理 1 中的(ii)式, 故 $b>1$ 时的方程(8)无解.

当 $b=1$ 时, 由(8)式可得 $d=3,r=1,(x_1,y_1)=$

$(2,1), s=1, \omega_0=0, 2\leqslant h\leqslant 2, \omega(3,2)=1, \omega(3,3)+\omega_0=r$, $\omega(3,3)$ 满足定理 1 中的(i)式，$3^{\frac{1-1}{2}}q^{\frac{n}{2}}=q^{\frac{n}{2}}=x_{2^1}\cdot(x_1y_1/2^s)=7$ 满足定理 1 中的(ii)式, 故 $b=1$ 时方程(8)仅有一组解 $(p,q,a,b,m,n)=(97,7,6,1,1,2)$.

由 (9) 式可得 $d=6, r=2, (x_1,y_1)=(5,2), s=1, \omega_0=1, h=2, \omega(6,2)=1, \omega(6,2)+\omega_0=r$, 这里由 $2\mid y_1$ 及 $y_1\mid 2^{(a-1)/2}\cdot 3^{(b-1)/2}\cdot q^{n/2}$ 得 $2\mid 2^{(a-1)/2}\cdot 3^{(b-1)/2}\cdot q^{n/2}$，因此 $(a-1)/2\geqslant 1$. $\omega(6,2)$ 满足定理 1 中的(i)式, $3^{(b-1)/2}q^{n/2}=x_{2^1}\cdot(x_1y_1/2^s)=7^2\cdot 5$ 不满足定理 1 的(ii)式，故方程(9)无解. 所以丢番图方程(1)仅有两组解 $(p,q,a,b,m,n)=(577,17,7,2,1,2),(97,7,6,1,1,2)$ 满足 $2\mid n$. 定理 2 证完.

参考文献:

[1] 施武杰. 关于单 K_4-群[J]. 科学通报, 1991, 36(12): 1281-1283.

[2] 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, 1998:195-196.

[3] 乐茂华, 徐广善. K_4-单群的几个 Diophantine 方程问题[J]. 中国科学: A 辑, 1996, 26(9):769-773.

[4] 袁平之. 几个未解决的不定方程问题[J]. 数学研究与评论, 2000, 20(4):627-628.

[5] Bilu Y, Hanrot G, Voutier P, et al. Existence of primitive divisors of Lucas and Lehmer numbers[J]. J Reine Angew Math, 2001, 539:75-122.

[6] 曹珍富. 不定方程及其应用[M]. 上海: 上海交通大学出版社, 2000:1-28.

On a Diophantine Equation in Single K_4-Group and it's Generalize

HE Zong-you

(Ningbo Scientz Biotechnology Co. Ltd., Ningbo 315013, China)

Abstract: For $p,q_i\in P, p>3, q_i>3, n_0,n_i,i,r\in N, n_0\geqslant 1, n_i\geqslant 1, 1\leqslant i\leqslant r, d\in N, d>0$ is not square number, in this paper, we study the solution $(p,q_1,q_2,\cdots,q_r,m,n_0,n_1,n_2,\cdots,n_r)$ of Diophantine equation $(p^m)^2-d\cdot(2^{n_0}q_1^{n_1}q_2^{n_2}\cdots q_r^{n_r})^2=1$, on using the theorem about the primitive divisors of Lucas number due to Bilu, Hanrot, Voutier, partially solve a diophantine equation in single K_4-group.

Key words: diophantine equation; Pell equation; solution; Lucas sequence; primitive divisor

（责任编辑　章践立）