关于不定方程 $x^2-3y^4=286$ *

朱 德 辉
(重庆师范大学 数学与计算机科学学院,重庆 400047)

摘　要 利用一种初等的证明方法,对不定方程 $x^2-3y^4=286$ 的正整数解进行了研究。证明过程中仅涉及到初等的数论知识,就是运用递归数列,同余式和平方剩余的方法。首先利用 Pell 方程的解的性质把不定方程 $x^2-3y^4=286$ 的解转化为由 4 个非结合类给出;对其每一种情况都利用递归数列,同余式和平方剩余的相关知识对其是否有正整数解进行证明,如果有正整数解并进行求解;最后得出该不定方程 $x^2-3y^4=286$ 仅有正整数解 $(x,y)=(17,1),(23,3)$。

关键词 平方剩余;递归数列;正整数解;不定方程
中图分类号 O156.1　　**文献标识码** A　　**文章编号** 1672-6693(2008)04-0030-03

关于不定方程 $x^2-Dy^4=N$(其中 D,N 为给定的整数,且 $D>0$ 为非平方数)已有不少研究工作[1-7]。设 $N(D,N)$ 是方程 $x^2-Dy^4=N$ 的正整数解的组数,Cohn[1] 证明了 $N(5,44)=1,(x,y)=(7,1)$;$N(5,11)=2,(x,y)=(4,1),(56,5)$;$N(5,-44)=3,(x,y)=(6,2),(19,3),(181,9)$ 这几个结果。Tzanakis[2] 证明了 $y\equiv 0(\mathrm{mod}8)$ 时,$N(2,17)=0$,$N(2,41)=0$,$N(8,17)=0$,$N(2,97)=0$。黎进香[6] 证明了 $N(3,46)=2,(x,y)=(7,1),(17,3)$。林丽娟[7] 证明了 $N(3,22)=2,(x,y)=(5,1),(85,7)$。

本文运用递归数列,同余式和平方剩余证明了不定方程 $x^2-3y^4=286$ 仅有正整数解 $(x,y)=(17,1),(23,3)$。

定理　不定方程

$$x^2-3y^4=286 \tag{1}$$

仅有正整数解 $(x,y)=(17,1),(23,3)$。

证明　首先考虑 Pell 方程 $a^2-3b^2=286$ 的一般解可由下面 4 个非结合类给出

$$a+b\sqrt{3}=\pm(17+\sqrt{3})(2+\sqrt{3})^n$$

或 $$a+b\sqrt{3}=\pm(-17+\sqrt{3})(2+\sqrt{3})^n$$

或 $$a+b\sqrt{3}=\pm(19+5\sqrt{3})(2+\sqrt{3})^n$$

或 $$a+b\sqrt{3}=\pm(-19+5\sqrt{3})(2+\sqrt{3})^n$$

令 $u_n\sqrt{3}+v_n=(\sqrt{3}+2)^n$,则如果(1)式有解,必有 n 使得 $y^2=\pm(v_n+17u_n)$

或 $y^2=\pm(-v_n+17u_n)=\mp(v_{-n}+17u_{-n})$

或 $y^2=\pm(5v_n+19u_n)$

或 $y^2=\pm(-5v_n+19u_n)=\mp(5v_{-n}+19u_{-n})$

当 $n\geqslant 0$ 时,$v_n+17u_n>0$,$5v_n+19u_n>0$;当 $n<0$ 时,$v_n+17u_n<0$,$5v_n+19u_n<0$。

因此可归结为

$$y^2=v_n+17u_n,n\geqslant 0 \tag{2}$$

或 $$y^2=-v_n+17u_n,n>0 \tag{3}$$

或 $$y^2=5v_n+19u_n,n\geqslant 0 \tag{4}$$

或 $$y^2=-5v_n+19u_n,n>0 \tag{5}$$

容易验证下列关系

$$v_{n+2}=4v_{n+1}-v_n,v_0=1,v_1=2$$

$$u_{n+2}=4u_{n+1}-u_n,u_0=0,u_1=1$$

$$\begin{cases}v_{2n}=v_n^2+3u_n^2=2v_n^2-1=6u_n^2+1\\ u_{2n}=2v_nu_n\\ v_{n+l}=3u_nu_l+v_nv_l\\ u_{n+l}=u_nv_l+v_nu_l\end{cases} \tag{6}$$

$$\begin{cases}u_{n+2kr}\equiv(-1)^ku_n(\mathrm{mod}v_r)\\ v_{n+2kr}\equiv(-1)^kv_n(\mathrm{mod}v_r)\\ u_{n+2kr}\equiv u_n(\mathrm{mod}u_r),v_{n+2kr}\equiv v_n(\mathrm{mod}u_r)\end{cases} \tag{7}$$

ⅰ)对(2)式取模 8,得剩余序列周期为 4,当 $n\equiv 1,2(\mathrm{mod}4)$ 时,$v_n+17u_n\equiv 3,3(\mathrm{mod}8)$ 为模 8 的

* 收稿日期:2008-03-20
资助项目:重庆市教委科研基金项目(No. KJ 050807)
作者简介:朱德辉(1981-),女,硕士研究生,研究方向为数论。

平方非剩余,故排除。剩 $n\equiv 0,3(\mathrm{mod}4)$,即 $n\equiv 0,3,4,7(\mathrm{mod}8)$。

对(2)式取模7,得剩余序列周期为8,当 $n\equiv 4,7(\mathrm{mod}8)$ 时,$v_n+17u_n\equiv 6,6(\mathrm{mod}7)$ 为模7的平方非剩余,故排除,剩 $n\equiv 0,3(\mathrm{mod}8)$ 即 $n\equiv 0,3,8,11(\mathrm{mod}16)$。

对(2)式取模97,得剩余序列周期为16,当 $n\equiv 3,11(\mathrm{mod}16)$ 时,$v_n+17u_n\equiv 87,10(\mathrm{mod}97)$ 为模97的平方非剩余,故排除,剩 $n\equiv 0,8(\mathrm{mod}16)$ 即 $n\equiv 0(\mathrm{mod}8)$。

对(2)式取模71,得剩余序列周期为7,当 $n\equiv 3,4,6(\mathrm{mod}7)$ 时,$v_n+17u_n\equiv 68,55,56(\mathrm{mod}71)$ 为模71的平方非剩余,故排除,剩 $n\equiv 0,1,2,5(\mathrm{mod}7)$,即 $n\equiv 0,1,2,5,7,8,9,12(\mathrm{mod}14)$。

对(2)式取模41,得剩余序列周期为14,当 $n\equiv 1,2,8,9(\mathrm{mod}14)$ 时,$v_n+17u_n\equiv 19,34,22,7(\mathrm{mod}41)$ 为模41的平方非剩余,故排除,剩 $n\equiv 0,5,7,12(\mathrm{mod}14)$ 即 $n\equiv 0,5,7,12,14,19,21,26(\mathrm{mod}28)$。又因为 $n\equiv 0(\mathrm{mod}8)$,可归结为 $n\equiv 0(\mathrm{mod}4)$,故排除 $n\equiv 5,7,14,19,21,26(\mathrm{mod}28)$,还剩 $n\equiv 0,12(\mathrm{mod}28)$,即 $n\equiv 0,12,28,40(\mathrm{mod}56)$。因为 $n\equiv 0(\mathrm{mod}8)$,故排除 $n\equiv 12,28(\mathrm{mod}56)$,还剩 $n\equiv 0,40(\mathrm{mod}56)$ 即 $n\equiv 0,40,56,96(\mathrm{mod}112)$。

对(2)式取模12065089,得剩余序列周期为112,当 $n\equiv 40,96(\mathrm{mod}112)$ 时,$v_n+17u_n\equiv 4738202,7326887(\mathrm{mod}12065089)$ 为模12065089的平方非剩余,故排除,剩 $n\equiv 0,56(\mathrm{mod}112)$,可归结为 $n\equiv 0(\mathrm{mod}56)$。

若 $n\neq 0$,令 $n=0+2(4k\pm 1)\times 7\times 2^t$

$$m=\begin{cases}2^t, t\equiv 0,1,3,4(\mathrm{mod}6)\\ 7\times 2^t, t\equiv 2,5(\mathrm{mod}6)\end{cases}$$

其中 $t>1$,由(7)式知

$$y^2=v_n+17u_n=v_{0+8km\pm 2m}+17u_{0+8km\pm 2m}\equiv v_{\pm 2m}+17u_{\pm 2m}\equiv \pm 17u_{2m}(\mathrm{mod}v_{2m})$$

易知 $v_{2m}\equiv 1(\mathrm{mod}8)$,设 $2^s\parallel u_m$,则

$$\left(\frac{u_m}{v_{2m}}\right)=\left(\frac{u_m/2^s}{v_{2m}}\right)=\left(\frac{v_{2m}}{u_m/2^s}\right)=\left(\frac{6u_m^2+1}{u_m/2^s}\right)=1$$

$$\left(\frac{v_m}{v_{2m}}\right)=\left(\frac{2v_m^2-1}{v_m}\right)=\left(\frac{-1}{v_m}\right)=1$$

所以 $$\left(\frac{u_{2m}}{v_{2m}}\right)=\left(\frac{2u_mv_m}{v_{2m}}\right)=\left(\frac{u_m}{v_{2m}}\right)\left(\frac{v_m}{v_{2m}}\right)=1$$

因此

$$1=\left(\frac{y^2}{v_{2m}}\right)=\left(\frac{\pm 17u_{2m}}{v_{2m}}\right)=\left(\frac{17}{v_{2m}}\right)\left(\frac{u_{2m}}{v_{2m}}\right)=\left(\frac{v_{2m}}{17}\right)\quad(8)$$

对 v_{2m} 模17得剩余序列周期为18,对 $2m$ 模18得剩余序列周期为6,且有表1。

表1 $2m$ 模18和 v_{2m} 模17情况下的数据

$t>1(\mathrm{mod}6)$	0	1	2	3	4	5
$2m(\mathrm{mod}18)$	2	4	2	16	14	16
$v_{2m}(\mathrm{mod}17)$	7	12	7	7	12	7

表中所有 $2m$ 均有 $\left(\frac{v_{2m}}{17}\right)=-1$,所以(8)式不成立,此时(2)式无解。

当 $n=0$ 时,得到方程(1)式的正整数解 $(x,y)=(17,1)$。

ⅱ)对(3)式取模71,得剩余序列周期为7,当 $n\equiv 0,2,5,6(\mathrm{mod}7)$ 时,$-v_n+17u_n\equiv 70,61,67,52(\mathrm{mod}71)$ 为模71的平方非剩余,故排除。剩 $n\equiv 1,3,4(\mathrm{mod}7)$,即 $n\equiv 1,3,4,8,10,11(\mathrm{mod}14)$。

对(3)式取模41,得剩余序列周期为14,当 $n\equiv 1,3,4,8,10,11(\mathrm{mod}14)$ 时,$-v_n+17u_n\equiv 15,24,35,26,17,6(\mathrm{mod}41)$ 为模41的平方非剩余,故排除。

由上得(3)式无解。

ⅲ)对(4)式取模8,得剩余序列周期为4,当 $n\equiv 0,1,2,3(\mathrm{mod}4)$ 时,$5v_n+19u_n\equiv 5,5,7,7(\mathrm{mod}8)$ 为模8的平方非剩余,故排除。

由此得(4)式无解。

ⅳ)对(5)式取模8,得剩余序列周期为4,当 $n\equiv 0,3(\mathrm{mod}4)$ 时,$-5v_n+19u_n\equiv 3,3(\mathrm{mod}8)$ 为模8的平方非剩余,故排除,还剩 $n\equiv 1,2(\mathrm{mod}4)$ 即 $n\equiv 1,2,5,6(\mathrm{mod}8)$。

对(5)式取模7,得剩余序列周期为8,当 $n\equiv 2,5(\mathrm{mod}8)$ 时,$-5v_n+19u_n\equiv 6,5(\mathrm{mod}7)$ 为模7的平方非剩余,故排除,还剩 $n\equiv 1,6(\mathrm{mod}8)$ 即 $n\equiv 1,6,9,14(\mathrm{mod}16)$。

对(5)式取模97,得剩余序列周期为16,当 $n\equiv 6,14(\mathrm{mod}16)$ 时,$-5v_n+19u_n\equiv 14,83(\mathrm{mod}97)$ 为模97的平方非剩余,故排除,还剩 $n\equiv 1,9(\mathrm{mod}16)$ 即 $n\equiv 1(\mathrm{mod}8)$。

对(5)式取模71,得剩余序列周期为7,当 $n\equiv 0,2,3,4,5,6(\mathrm{mod}7)$ 时,$-5v_n+19u_n\equiv 66,41,13,11,31,42(\mathrm{mod}71)$ 为模71的平方非剩余,故排除,还剩 $n\equiv 1(\mathrm{mod}7)$。

对(5)式取模3,得剩余序列周期为6,当 $n\equiv 2$,

$3 \pmod 6$ 时，$-5v_n+19u_n \equiv 2, 2 \pmod 3$ 为模 3 的平方非剩余，故排除，还剩 $n \equiv 0,1,4,5 \pmod 6$ 即 $n \equiv 0,1,4,5,6,7,10,11 \pmod{12}$。

对(5)式取模 13，得剩余序列周期为 12，当 $n \equiv 0,4,6,10 \pmod{12}$ 时，$-5v_n+19u_n \equiv 8,7,5,6 \pmod{13}$ 为模 13 的平方非剩余，故排除，还剩 $n \equiv 1,5,7,11 \pmod{12}$ 即 $n \equiv 1,5,7,11,13,17,19,23 \pmod{24}$。

对(5)式取模 193，得剩余序列周期为 24，当 $n \equiv 5,11,17,23 \pmod{24}$ 时，$-5v_n+19u_n \equiv 38,29,155,164 \pmod{193}$ 为模 193 的平方非剩余，故排除，还剩 $n \equiv 1,7,13,19 \pmod{24}$。

又由于 $n \equiv 1 \pmod 8$，故排除 $n \equiv 7,13,19 \pmod{24}$，还剩 $n \equiv 1 \pmod{24}$。由 $n \equiv 1 \pmod 8$，$n \equiv 1 \pmod 7$，$n \equiv 1 \pmod{24}$ 即 $n \equiv 1 \pmod{168}$。

若 $n \neq 1$，令 $n = 1+2(4k \pm 1)\times 3 \times 7 \times 2^t$

$$m = \begin{cases} 2^t, t \equiv 0,1,3,5,6,8 \pmod{10} \\ 3 \times 2^t, t \equiv 2,7 \pmod{10} \\ 7 \times 2^t, t \equiv 4,9 \pmod{10} \end{cases}$$

其中 $t > 1$，由(6)，(7)式知

$$y^2 = -5v_n + 19u_n =$$
$$-5v_{1+8km\pm 2m} + 19u_{1+8km\pm 2m} \equiv -5v_{1\pm 2m} + 19u_{1\pm 2m} \equiv$$
$$-5(3u_1u_{\pm 2m} + v_1v_{\pm 2m}) + 19(u_1v_{\pm 2m} + v_1u_{\pm 2m}) \equiv$$
$$23u_{\pm 2m} + 9v_{\pm 2m} \equiv \pm 23u_{2m} \pmod{v_{2m}}$$

又由 ⅰ) 知 $\left(\frac{u_{2m}}{v_{2m}}\right) = 1$，所以

$$1 = \left(\frac{y^2}{v_{2m}}\right) = \left(\frac{\pm 23u_{2m}}{v_{2m}}\right) = \left(\frac{v_{2m}}{23}\right) \qquad (9)$$

对 v_{2m} 模 23 得剩余序列周期为 11，而 $2m$ 模 11 得剩余序列周期为 10 且有表 2。

表 2 $2m$ 模 11 和 v_{2m} 模 23 情况下的数据

$t > 1 \pmod{10}$	0	1	2	3	4	5	6	7	8	9
$2m \pmod{11}$	2	4	2	5	4	9	7	9	6	7
$v_{2m} \pmod{23}$	7	5	7	17	5	7	5	7	17	5

表中所有 $2m$ 均有 $\left(\frac{v_{2m}}{23}\right) = -1$，所以(9)式不成立，此时(5)式无解。

当 $n = 1$ 时，得到方程(1)式的正整数解 $(x,y) = (23,3)$。

综合 ⅰ) ~ ⅳ) 知方程(1)式仅有正整数解 $(x,y) = (17,1),(23,3)$。 证毕

参考文献：

[1] COHN J H E. Some Quartic Diophantine Equations[J]. Pacific J Math, 1986, 26: 233-243.

[2] TZANAKIS N. On the Diophantine Equations $y^2 - D = 2^n$ [J]. J Number Theory, 1983, 17: 144-164.

[3] 曹珍富. 丢番图方程引论[M]. 哈尔滨: 哈尔滨工业大学出版社, 1989.

[4] 柯召, 孙琦. 数论讲义[M]. 北京: 高等教育出版社, 2001.

[5] 罗明. 关于不定方程 $x^3+1=7y^2$[J]. 重庆师范学院学报(自然科学版), 2003, 20(1): 5-7.

[6] 林丽娟, 何波. 关于不定方程 $x^3-3y^4=22$[J]. 重庆师范大学学报(自然科学版), 2007, 24(3): 31-32.

[7] 姚益民. Moisil-Theodorsco 方程组的 Riemann 边值问题[J]. 四川师范大学学报(自然科学版), 2006, 29(2): 188-191.

On the Diophantine Equation $x^2 - 3y^4 = 286$

ZHU De-hui

(College of Mathematics and Computer Science, Chongqing Normal University, Chongqing 400047, China)

Abstract: The positive integral solutions to the diophantine equation $x^2 - Dy^4 = N$ (D and N are the given integers, $D>0$ and D is non-square) is an old problem which, until now, cannot be resolved completely. The study of the diophantine equation $x^2 - Dy^4 = N$ (D and N are the given integers, $D>0$ and D is non-square) has caused some authors´ interest, such as Cohn, Tzanakis, LI Jin-xiang, LIN Li-juan. Cohn has proven some conclusions. For example: $N(5,44)=1$, $(x,y)=(7,1)$; $N(5,11)=2$, $(x,y)=(4,1),(56,5)$; $N(5,-44)=3$, $(x,y)=(6,2),(19,3),(181,9)$. Tzanakis has proven some conclusions while $y \equiv 0 \pmod 8$. For example: LI Jin-xiang has proven one conclusion: $N(3,46)=2$, $(x,y)=(7,1),(17,3)$. LIN Li-juan also has proven one conclusion: $N(3,22)=2$, $(x,y)=(5,1),(85,7)$. But this diophantine equation $x^2-3y^4=286$ still has not been solved until now. In this paper the author has proved that the diophantine equation $x^2-3y^4=286$ has only positive integral solution $(x,y)=(17,1),(23,3)$ with the primary methods of recursive sequence, quadratic remainder and congruence.

Key words: quadratic residue; recurrent sequence; positiue integral solution; diophantine equation

(责任编辑 黄 颖)