DOI:10.3969/J. ISSN. 1672-6693.2010.03.010

关于丢番图方程 $x^3+1=57y^2$*

段辉明
(重庆邮电大学 数理学院,重庆 400065)

摘要 利用初等的证明方法即同余法、Pell 方程的整数解的性质、Maple 小程序以及递归序列和二次剩余的方法,对一个丢番图方程 $x^3+1=57y^2$ 的整数解进行了研究。证明过程中仅涉及到初等的数论知识,首先利用等式的性质把原丢番方程的解转化为 4 种情形进行讨论,对其第一种利用等式的性质得出无整数解,第二种情形利用同余式得出无整数解,后面两种利用同余式递归数列和平方剩余的相关知识以及 maple 小程序得出整数解和平凡解;最后综合得该丢番图方程仅有整数解 $(x,y)=(-1,0),(8,\pm3)$。

关键词 丢番图方程;整数解;递归序列;平方剩余
中图分类号 O156.1 **文献标识码** A **文章编号** 1672-6693(2010)03-0041-03

关于丢番图方程 $x^3\pm1=Dy^2$ $(D>0)$ 已有不少的研究工作。当 D 无 $6k+1$ 的素因数时,其全部整数解已由柯召等人得到[1]。但当 D 有 $6k+1$ 的素因数时,方程的求解较为困难。此类方程有非平凡解时求解更困难。1999 年,倪谷炎[2] 在关于不定方程 $x^3+1=Dy^2$ 一文中指出当 $0<D<100$,不含平方因子,且被 $6k+1$ 型的素数整除时,只有当 $D=7,14,35,37,38,57,65,86$ 时有非平凡解,但没有证明。后来当 $D=7,14,35,37,38,57,65,86$ 时,分别由罗明[3-4] 与笔者[5-8] 解决,其余当 $D=37,57$ 都未被解决,本文解决的是 $D=57$ 的全部整数解。

引理 1[1] 不定方程 $4x^4-3y^2=1$ 有整数解 $(x,y)=(1,1),(-1,-1),(1,-1),(-1,1)$。

定理 丢番图方程

$$x^3+1=57y^2 \tag{1}$$

仅有整数解 $(x,y)=(-1,0),(8,\pm3)$。

证明 因为 $(x+1,x^2-x+1)=1$ 或 3,故原不定方程(1)式给出下列 4 种可能的分解。

情形Ⅰ $x+1=57u^2,x^2-x+1=v^2,y=uv$

情形Ⅱ $x+1=3u^2,x^2-x+1=19v^2,y=uv$

情形Ⅲ $x+1=u^2,x^2-x+1=57v^2,y=uv$

情形Ⅳ $x+1=19u^2,x^2-x+1=3v^2,y=uv$

以下对这 4 种情形分别讨论原丢番图方程的整数解。

情形Ⅰ 解其中的第二个式子 $x=0,1$ 得,均不适合第一式,故无解。

情形Ⅱ 由此情形中的前一个式子知 $x\equiv-1\pmod 3$,再由后式得

$$19v^2\equiv x^2-x+1\pmod 3$$

即 $3\mid v$,从而 $x^2-x+1\equiv0\pmod 9$,所以 $(2x-1)^2+3\equiv0\pmod 9$,但 $2x-1\equiv0\pmod 3$,即 $(2x-1)^2\equiv0\pmod 9$,从而 $3\equiv0\pmod 9$,矛盾。

情形Ⅲ 将此情形中的第二式变为 $(2x-1)^2-57(2v)^2=-3$,因为方程 $x^2-57y^2=-3$ 的全部整数解,由以下[9] 结合类给出

$$\pm(x_n+y_n\sqrt{57})=\pm(15+2\sqrt{57})(u_n+v_n\sqrt{57})=\pm(15+2\sqrt{57})(151+20\sqrt{57})^n,n\in\mathbf{Z}$$

其中 $15+2\sqrt{57}$ 是方程 $x^2-57y^2=-3$ 的最小正整数解,而 pell 方程 $x^2-57y^2=1$ 的通解为 $\pm(u_n+v_n\sqrt{57})=\pm(151+20\sqrt{57})^n$。

故得 $2x-1=\pm(15u_n+114v_n),n\in\mathbf{Z}$

因为 $3\mid u$,令 $u=3z$,则 $x=9z^2-1$,代入上式得

$$18z^2=\pm(15u_n+114v_n)+3,n\in\mathbf{Z}$$

即 $$6z^2=\pm(5u_n+38v_n)+1,n\in\mathbf{Z}$$

由于 $5u_{-n-1}+38v_{-n-1}=5u_{n+1}-38v_{n+1}=5(151u_n+1140v_n)-38(20u_n+151v_n)=-(5u_n+38v_n)$

所以只须考虑

$$6z^2=5u_n+38v_n+1,n\in\mathbf{Z} \tag{2}$$

容易验证下列关系式成立

$$u_{n+2}=302u_{n+1}-u_n,u_0=1,u_1=151 \tag{3}$$

$$v_{n+2}=302u_{n+1}-v_n,v_0=0,v_1=20 \tag{4}$$

* 收稿日期:2009-07-05
资助项目:重庆邮电大学自然科学基金(No. A20080-40)
作者简介:段辉明,女,讲师,硕士,研究方向为数论。

$u_{n+2k}\equiv -u_n \pmod{u_k}$,$v_{n+2k}\equiv -v_n \pmod{u_k}$ (5)

据此有以下引理。

引理2 只有当 $n\equiv 0 \pmod{11\ 088}$,(2)式才成立。

证明 当 $n\equiv 1,2 \pmod 3$ 时,$6z^2=5u_n+38v_n+1\equiv 1,2 \pmod 3$ 不可能成立,所以必须考虑 $n\equiv 0 \pmod 3$,等价于 $n\equiv 0,3 \pmod 6$。

对递归序列 $\{5u_n+38v_n+1\}$ 取 mod 43,剩余类序列周期为6,当 $n\equiv 3 \pmod 6$ 时,$5u_n+38v_n+1\equiv 39 \pmod{43}$,因为 $1=\left(\frac{6z^2}{43}\right)=\left(\frac{39}{43}\right)=-1$,矛盾,所以 $n\equiv 0 \pmod 6$,等价于 $n\equiv 0,6,12 \pmod{18}$。

对递归序列 $\{5u_n+38v_n+1\}$ 取 mod 27 542 701,剩余类序列周期为18,当 $n\equiv 6,12 \pmod{18}$ 时

$$5u_n+38v_n+1\equiv 457\ 526,27\ 085\ 172 \pmod{27\ 542\ 701}$$

同理利用 Jacobi 符号得到矛盾的式子,所以 $n\equiv 0 \pmod{18}$。

下证 $n\equiv 0 \pmod{112}$,同理,取 mod 27 634 207,剩余类序列周期为7,当 $n\equiv 3,5 \pmod 7$ 时

$$5u_n+38v_n+1\equiv 1,27\ 632\ 693 \pmod{27\ 634\ 207}$$

所以 $n\equiv 0,1,2,4,6 \pmod 7$,等价于

$$n\equiv 0,1,2,4,6,7,8,9,11,13 \pmod{14}$$

取 mod 13,剩余类序列周期为14,当 $n\equiv 2,4,7,13 \pmod{14}$ 时

$$5u_n+38v_n+1\equiv 4,4,9,9 \pmod{13}$$

剩下 $n\equiv 0,1,6,8,9,11 \pmod{14}$。取 mod 2 111 677,剩余类序列周期为14,当 $n\equiv 1,8 \pmod{14}$

$$5u_n+38v_n+1\equiv 1516,2\ 110\ 163 \pmod{2\ 111\ 677}$$

剩下 $n\equiv 0,6,9,11 \pmod{14}$,等价于 $n\equiv 0,6,9,11,14,20,23,25 \pmod{28}$。

取 mod 29,剩余类序列周期为28,当 $n\equiv 6,20,23 \pmod{28}$ 时

$$5u_n+38v_n+1\equiv 10,21,11 \pmod{29}$$

剩下 $n\equiv 0,9,11,14,25 \pmod{28}$。取 mod 83,剩余类序列周期为28,当 $n\equiv 9,11 \pmod{28}$ 时

$$5u_n+38v_n+1\equiv 59,30 \pmod{83}$$

剩下 $n\equiv 0,14,25 \pmod{28}$。取 mod 315 160 829 143,剩余类周期为28,当 $n\equiv 25 \pmod{28}$ 时

$$5u_n+38v_n+1\equiv 315\ 160\ 371\ 619 \pmod{315\ 160\ 829\ 143}$$

剩下 $n\equiv 0,14 \pmod{28}$。等价于 $n\equiv 0,14,28,42 \pmod{56}$。

取 mod 281,剩余类序列周期为56,当 $n\equiv 28,42 \pmod{56}$ 时,$5u_n+38v_n+1\equiv 277,218 \pmod{281}$,剩下 $n\equiv 0,14 \pmod{56}$。取 mod 34 273,剩余类序列周期为56,当 $n\equiv 14 \pmod{56}$ 时,$5u_n+38v_n+1\equiv 14\ 296 \pmod{34\ 273}$,剩下 $n\equiv 0 \pmod{56}$,等价于 $n\equiv 0,56 \pmod{112}$。

取 mod 192 977,剩余类序列周期为112,当 $n\equiv 56 \pmod{112}$ 时

$$5u_n+38v_n+1\equiv 192\ 973 \pmod{192\ 977}$$

剩下 $n\equiv 0 \pmod{112}$。

取 mod 13 691,剩余类序列周期为11,当 $n\equiv 1,2,3,4,6,7,9 \pmod{11}$ 时,$5u_n+38v_n+1\equiv 1\ 516,8\ 099,6\ 281,9\ 041,4\ 580,7\ 340,12\ 105 \pmod{13\ 619}$,剩下 $n\equiv 0,5,8,10 \pmod{11}$。取 mod 939 377,剩余类序列周期为11,当 $n\equiv 5,8,10 \pmod{11}$ 时,$5u_n+38v_n+1\equiv 1,481\ 853,939\ 373 \pmod{939\ 377}$,剩下 $n\equiv 0 \pmod{11}$。又因为 $n\equiv 0 \pmod{18}$,$n\equiv 0 \pmod{112}$,所以 $n\equiv 0 \pmod{11\ 088}$。 证毕

引理3 设 $n\equiv 0 \pmod{11\ 088}$,只有当 $n=0$ 时,(2)式成立。

证明 当 $n\equiv 0 \pmod{11\ 088}$ 且 $n\neq 0$,令 $n=2\times 2^t\times 3\times 3\times 7\times 11\times k$,其中 $k\equiv 1 \pmod 2$,$t\geqslant 3$,现对 k 分两种情形讨论。

当 $k\equiv 1 \pmod 4$,令

$$m=\begin{cases}9\times 2^t, t\equiv 0 \pmod 4\\ 7\times 11\times 2^t, t\equiv 1 \pmod 4\\ 2^t, t\equiv 2 \pmod 4\\ 3\times 11\times 2^t, t\equiv 3 \pmod 4\end{cases}$$

$m\equiv 24 \pmod{40}$ 由(3)~(5)式得

$$6z^2\equiv 38v_{2m}+1 \pmod{u_{2m}}$$

又注意当

$$m\equiv 0 \pmod 2,\ u_m\equiv 1 \pmod 8,\ v_m\equiv 0 \pmod 8$$

以及 $u_m^2+57v_m^2\equiv 1 \pmod 8$,于是有

$$\left(\frac{38v_{2m}+1}{u_{2m}}\right)=\left(\frac{76u_mv_m+u_m^2-57v_m^2}{u_m^2+57v_m^2}\right)=\left(\frac{2u_m^2+76u_mv_m}{u_m^2+57v_m^2}\right)=$$

$$\left(\frac{2u_m}{u_m^2+57v_m^2}\right)\left(\frac{u_m+38v_m}{u_m^2+57v_m^2}\right)=\left(\frac{-1}{u_m}\right)\left(\frac{u_m+38v_m}{u_m^2+57v_m^2}\right)=$$

$$\left(\frac{-1}{u_m}\right)\left(\frac{(38v_m)^2+57v_m^2}{u_m+38v_m}\right)=\left(\frac{1\ 501}{u_m+38v_m}\right)=\left(\frac{19\times 79}{u_m+38v_m}\right)=$$

$$\left(\frac{79}{u_m+38v_m}\right)\text{(因为 } u_m+38v_m\equiv 1 \pmod{19},$$

$$u_m+38v_m\equiv 1 \pmod 4\text{)}=\left(\frac{u_m+38v_m}{79}\right)$$

利用递归数列 $\{u_m+38v_m\}$,取 mod 79,得周期为40的剩余类序列。根据 m 的取法,同时注意 $\{t'\}$ 到对 mod 40 有周期4,因为 $m\equiv 24 \pmod{40}$ 有,

$u_m+38v_m\equiv 33\pmod{79}$ 所以由(2)式得

$$1=\left(\frac{6z^2}{u_m^2+57v_m^2}\right)=\left(\frac{u_m+38v_m}{79}\right)=\left(\frac{33}{79}\right)=-1$$

矛盾。

当 $k\equiv -1\pmod 4$ 令

$$m=\begin{cases}2^t, t\equiv 0\pmod 4\\ 3\times 11\times 2^t, t\equiv 1\pmod 4\\ 9\times 2^t, t\equiv 2\pmod 4\\ 7\times 11\times 2^t, t\equiv 3\pmod 4\end{cases}$$

$m\equiv 16\pmod{40}$，由(3)～(5)式得

$$6z^2\equiv -38v_{2m}+1\pmod{u_{2m}}$$

类似地，有

$$\left(\frac{-38v_{2m}+1}{u_{2m}}\right)=\left(\frac{-76u_mv_m+u_m^2-57v_m^2}{u_m^2+57v_m^2}\right)=\left(\frac{79}{u_m-38v_m}\right)=\left(\frac{u_m+38v_m}{79}\right)$$

对递归数列 $\{u_m-38v_m\}$，取 mod 79 得周期为 40 的剩余类序列。根据 m 的取法，同时注意到 $\{2^t\}$ 对 mod 40 的周期为 4，因为 $m\equiv 16\pmod{40}$，有 $u_m-38v_m\equiv 33\pmod{79}$，所以由(2)式得

$$1=\left(\frac{6z^2}{u_m^2+57v_m^2}\right)=\left(\frac{u_m-38v_m}{79}\right)=\left(\frac{33}{79}\right)=-1$$

矛盾。

当 $n=0$ 成立，给出了(1)式的一组整数解 $(x,y)=(8,\pm 3)$。　　证毕

情形Ⅳ　此情形中的第二式 $(2x-1)^2-3(2v)^2=-3$，$(2v)^2-3\left(\frac{2x-1}{3}\right)^2=1$，即 $(2v)^2-3\left(\frac{38u^2-3}{3}\right)^2=1$，又 $3\mid u$，令 $u=3z$ 得 $(2v)^2-3(114z^2-1)^2=1$，因此

$$|2v|+(114z^2-1)\sqrt{3}=(u_n+v_n\sqrt{3})=(2+\sqrt{3})^n, n\in\mathbf{Z}$$

其中 $2+\sqrt{3}$ 是 Pell 方程 $x^2-3y^2=1$ 的基本解，所以 $114z^2=v_n+1, n\in\mathbf{Z}$。因为 $2\mid n$ 时，$2\mid v_n$，所以 $114u^2=v_n+1$ 不可能成立，故必须考虑 $n\equiv 1\pmod 2$，以下分两种情况讨论。

令 $n=4m-1$，有

$$114z^2=v_{4m-1}+1=-u_{4m}+2v_{4m}+1=-(1+6v_{2m}^2)+4u_{2m}v_{2m}+1=2v_{2m}(2u_{2m}-3v_{2m})=2v_{2m}u_{2m-1}$$

所以　　$57z^2=v_{2m}u_{2m-1}$

因为　　$(v_{2m},u_{2m-1})=(v_{2m},2u_{2m}-3v_{2m})=(2u_{2m},v_{2m})=(v_{2m},2)=2$

而 3 不整除 u_{2m-1}，故得

$$u_{2m-1}=2a^2, v_{2m}=114b^2 \quad (6)$$

或

$$u_{2m-1}=38a^2, v_{2m}=6b^2 \quad (7)$$

其中 $u=2ab$。

(6)式的前式代入 $u_{2m-1}^2-3v_{2m-1}^2=1$ 得，$4a^2-3v_{2m-1}^2=1$，由引理 1 得：$v_{2m-1}=\pm 1$，即 $m=0$ 或 1，但当 $m=1$ 时不适合(6)式的后一个式子，而当 $m=0$ 时(6)式中 $b=0$ 从而 $u=0$，这就给出了(1)式的平凡解 $(x,y)=(-1,0)$。

(7)式的后一个式子得：$u_mv_m=b^2$，而 3 不整除 u_m，于是 $u_m=c^2, v_m=2d^2, b=cd$，从而 $c^4-3(d^2)^2=1$，根据方程 $x^4-Dy^2=1$[9] 的结果，必有 $d=0$，从而 $b=0, v_{2m}=0, m=0$。但不适合(7)式的前一个式子，故(7)式无解。

同理，令　　$n=4m+1$

$$114z^2=v_{4m+1}+1=u_{4m}+2v_{4m}+1=2u_{2m}(u_{2m}+2v_{2m})=2u_{2m}v_{2m+1}$$

所以　　$57z^2=u_{2m}v_{2m+1}$

因为　　$(u_{2m},v_{2m+1})=(u_{2m},u_{2m}+2v_{2m})=(u_{2m},2v_{2m})=(u_{2m},2)=1$

注意到 3 不整除 u_{2m} 故得

$$u_{2m-1}=a^2, v_{2m}=57b^2 \quad (8)$$

或

$$u_{2m-1}=19a^2, v_{2m}=3b^2 \quad (9)$$

(8)式的前一个式子代入 $u_{2m}^2-3v_{2m}^2=1$ 得，$4a^2-3v_{2m}^2=1$，是已经解决的方程[9] 的结果，可得 $v_{2m}=0$，即 $m=0$，将 $m=0$ 代入 $114z^2=v_{4m+1}+1$ 式得 $114z^2=v_1+1=2$，不可能成立。

(9)式的后一个式子代入 $u_{2m+1}^2-3v_{2m+1}^2=1$ 得 $u_{2m+1}^2-27b^2=1$，根据方程 $x^2-Dy^4=1$[1] 的结果，必有 $b=0$，从而 $u_{2m+1}=1$ 不可能成立，即(9)式无解。

综合 4 种情形的结果知，方程(1)式仅有整数解 $(x,y)=(-1,0), (8,\pm 3)$。　　证毕

参考文献：

[1] 曹珍富. 丢番图方程引论[M]. 哈尔滨：哈尔滨工业大学出版社，1989：209-213.

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

[3] 罗明. 关于不定方程 $x^3\pm 1=14y^2$[J]. 重庆师范学院学报(自然科学学版)，1995(3)：112-115.

[4] 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(1)：5-7.

[5] 段辉明，一个未解决的丢番图方程 $x^3+1=35y^2$[J]. 高师理科学刊，2005(2)：5-7.

[6] 段辉明. 关于不定方程 $x^3+1=38y^2$ [J]. 华东师范大学学报(自然科学版),2006(1):35-39.
[7] 段辉明. 关于不定方程方程 $x^3+1=86y^2$ [J]. 高师理科学刊,2007(2):3-5.
[8] 段辉明,罗燕. 关于丢番图方程 $x^3+1=65y^2$. 贵州师范学院学报(自然科学版),2008(1):6-8.
[9] 柯召,孙琦. 谈谈不定方程[M]. 上海:上海教育出版社,1980:28-35.

On the Diophantine Equation $x^3+1=57y^2$

DUAN Hui-ming

(College of Mathematics and Physics, Chongqing University of Post and Telecommunications, Chongqing 400065, China)

Abstract: In this paper the author studies all the integer solutions to the diophantine equation $x^3+1=57y^2$. The process is as follows: classify the will-be integer solutions to the diophantine equation into four equations by equation firstly, then take models on these equations, the first equation and second equantion aren't integer solutions. At last two equations are integer solutions, at the same time, the methods of recursive sequences and maple formality and Pell equation and quadratic remainder are used. At last, it is proved that the diophantine equation $x^3+1=57y^2$ has only positive integer solutions $(x,y)=(-1,0),(8,\pm 3)$.

Key words: Diophantine equation; integer solution; recurrent sequence; guadratic remaider

(责任编辑 黄 颖)