文章编号:1672 -058X(2013)03 -0017 -05

不定方程 $y^2 = x^3 - 13$ 的初等解法

熊 军[1],敬 勇[2]
(1. 重庆育才中学,重庆 400050;2. 西南财经大学 数学系,成都 610074)

摘 要:给出了不定方程 $y^2 = x^3 - 13$ 仅有解 $x = 17, y = \pm 70$ 的初等解法.

关键词:不定方程;初等解法;本原解
中图分类号:O156. 7 **文献标志码**:A

利用代数数论知识[1-2],易知不定方程

$$y^2 = x^3 - 13$$

仅有解 $x = 17, y = \pm 70$. 下面避开代数数论,给出它的初等解法.

先作一些准备工作. 考察不定方程

$$x^2 + 13y^2 = n \tag{1}$$

其中 $n \in Z^+, n > 13$ 并且 $(n, 13) = 1$.

若 $\{x_1, y_1\}$ 为式(1)的解,满足 $(x_1, y_1) = 1$,则称 $\{x_1, y_1\}$ 为式(1)的本原解.

引理 1 若式(1)有本原解,则同余方程

$$S^2 \equiv -13 \pmod n \tag{2}$$

有解.

证明 令 $\{x_1, y_1\}$ 是式(1)的一组本原解,则 $(x_1 y_1, n) = 1$,于是同余方程

$$S y_1 \equiv x_1 \pmod n$$

有解,因此 $S^2 y_1^2 \equiv x_1^2 \equiv -13y^2 \pmod n$,从而 $S^2 \equiv -13 \pmod n$. 引理 1 证毕.

引理 2 令 $m > 1, (a, m) = 1$,则二元一次同余方程

$$au + v \equiv 0 \pmod m \tag{3}$$

必有解 u_0, v_0,满足

$$0 < |u_0| \leqslant \sqrt{m}, 0 < |v_0| < \sqrt{m}$$

证明 考虑集合 $au + v$, u 的取值范围是

$$0 \leqslant u \leqslant \sqrt{m} \tag{4}$$

v 的取值范围是

$$\begin{cases} 0 \leqslant v \leqslant \sqrt{m}, \text{当 } m \text{ 不是平方数} \\ 0 \leqslant v \leqslant \sqrt{m} - 1, \text{当 } m \text{ 是平方数} \end{cases} \tag{5}$$

则这个集合的元素个数是

收稿日期:2012 -11 -01;**修回日期**:2012 -11 -18.

作者简介:熊军(1965-),男,重庆铜梁人,从事高中数学教学理论研究.

$$K=\begin{cases}(\sqrt{m}+1)^2>m,\text{当 } m \text{ 不是平方数}\\ \sqrt{m}(\sqrt{m}+1)>m,\text{当 } m \text{ 是平方数}\end{cases}$$

因此,由抽屉原则,必有两组不同的$\{v_1,u_1\}$,$\{v_2,u_2\}$,使得 $au_1+v_1\equiv au_2+v_2(\bmod m)$. 现取 $u_0=u_1-u_2$,$v_0=v_1-v_2$,显然 u_0,v_0 不同时为零满足式(3). 由式(4)知 $|u_0|\leqslant\sqrt{m}$;由式(5)知 $|v_0|<\sqrt{m}$;此外,若 $u_0=0$,则 $v_0\neq0$;但 u_0,v_0 满足式(3)推出 $m|v_0$,因此 $|v_0|\geqslant m$,但这和 $|v_0|\leqslant m$ 矛盾,所以 $u_0\neq0$. 同理,若 $v_0=0$,则 $u_0\neq0$;进而由 u_0,v_0 满足式(3)及 $(a,m)=1$ 推出 $m|u_0$,因此 $|u_0|\geqslant m$,但这和 $|u_0|\leqslant m$,$m>1$ 矛盾,所以,$v_0\neq0$. 引理 2 证毕.

引理 3 若式(2)有解 $S_1(\bmod n)$,则不定方程(1)有一组本原解$\{x_1,y_1\}$,满足

$$S_1,y\equiv x_1(\bmod n) \tag{6}$$

证明 显然有$(S_1,n)=1$,因而由引理 2 知,必有 u_0,v_0 满足

$$0<|u_0|\leqslant\sqrt{n},0<|v_0|<\sqrt{n} \tag{7}$$

$$S_1u_0\equiv v_0(\bmod n) \tag{8}$$

由式(7),得 $14\leqslant v_0^2+13u_0^2<14n$. 由 S_1 满足式(2)及式(8),得 $v_0^2+13u_0^2\equiv0(\bmod n)$. 于是得

$$v_0^2+13u_0^2=kn\quad(1\leqslant k\leqslant13,k\in Z^+) \tag{9}$$

若 $k=1$,$\{v_0,u_0\}$是式(1)的解. 下证 $d=(v_0,u_0)=1$. 由式(9)得 $d|n$;再由式(8)得 $S_1\left(\frac{u_0}{d}\right)\equiv\left(\frac{v_0}{d}\right)\left(\bmod \frac{n}{d}\right)$. 因而 $\frac{n}{d^2}=\left(\frac{v_0}{d^2}\right)^2+13\left(\frac{u_0}{d^2}\right)^2\equiv S_1^2\left(\frac{u_0}{d}\right)^2+13\left(\frac{u_0}{d_2}\right)^2\equiv0\left(\bmod \frac{n}{d}\right)$. 这里用到了 $S_1^2\equiv-13\left(\bmod \frac{n}{d}\right)$,且当且仅当 $d=1$ 时成立,所以$\{v_0,u_0\}$是式(1)的本原解.

若 $k=2$,则式(1)无解. 若式(1)有解,考虑方程组

$$\begin{cases}x^2+13y^2=n\\ v_0^2+13u_0^2=2n\end{cases}$$

则存在 a,b 满足 $a^2+13b^2=2n^2$,有 $S^2\equiv2n^2(\bmod 13)$,从而勒让德符号$\left(\frac{2n^2}{13}\right)=\left(\frac{2}{13}\right)=1$,这与$\left(\frac{2}{13}\right)=-1$ 矛盾. 故 $k\neq2$.

同理,由勒让德符号$\left(\frac{5}{13}\right)=\left(\frac{7}{13}\right)=\left(\frac{8}{13}\right)=\left(\frac{11}{13}\right)=\left(\frac{6}{13}\right)=-1$ 知,$k\neq5,6,7,8,11$.

若 $k=3$,即 $v_0^2+13u_0^2=3n$,则 $v_0^2+13u_0^2\equiv v_0^2+u_0^2\equiv0(\bmod 3)$,故有

$\begin{cases}v_0^2\equiv0(\bmod 3)\\ u_0^2\equiv0(\bmod 3)\end{cases}$ 或 $\begin{cases}v_0^2\equiv1(\bmod 3)\\ u_0^2\equiv2(\bmod 3)\end{cases}$ 或 $\begin{cases}v_0^2\equiv2(\bmod 3)\\ u_0^2\equiv1(\bmod 3)\end{cases}$. 由勒让德符号$\left(\frac{2}{3}\right)=-1$,知 $S^2\equiv2(\bmod 3)$ 无解,$\begin{cases}v_0^2\equiv0(\bmod 3)\\ u_0^2\equiv0(\bmod 3)\end{cases}$ 从而$\begin{cases}v_0\equiv0(\bmod 3)\\ u_0\equiv0(\bmod 3)\end{cases}$ 即 $3|d$,$d=(v_0,u_0)\geqslant3$.

由式(9)得 $d^2|3n$. 再由式(8)得 $S_1\left(\frac{u_0}{d}\right)\equiv\left(\frac{v_0}{d}\right)\left(\bmod \frac{3n}{d}\right)$. 因而$\frac{3n}{d^2}=\left(\frac{v_0}{d^2}\right)^2+13\left(\frac{u_0}{d^2}\right)^2\equiv S_1^2\left(\frac{u_0}{d}\right)^2+13\left(\frac{u_0}{d^2}\right)^2\equiv0\left(\bmod \frac{3n}{d}\right)$.

这里用到了 $S_1^2\equiv-13\left(\bmod \frac{3n}{d}\right)$,且仅当 $d=1$ 时成立,矛盾. 故 $k\neq3$.

若 $k=4$,即 $v_0^2+13u_0^2=4n$,则 $v_0^2+13u_0^2\equiv v_0^2+u_0^2\equiv0(\bmod 4)$,故有

$$\begin{cases}v_0^2\equiv 0(\bmod 4)\\u_0^2\equiv 0(\bmod 4)\end{cases}\text{或}\begin{cases}v_0^2\equiv 1(\bmod 4)\\u_0^2\equiv 3(\bmod 4)\end{cases}\text{或}\begin{cases}v_0^2\equiv 2(\bmod 4)\\u_0^2\equiv 2(\bmod 4)\end{cases}\text{或}\begin{cases}v_0^2\equiv 3(\bmod 4)\\u_0^2\equiv 1(\bmod 4)\end{cases}$$

显然 $S^2\equiv2(\bmod 4)$ 和 $S^2\equiv3(\bmod 4)$ 无解,于是 $\begin{cases}v_0^2\equiv0(\bmod 4)\\u_0^2\equiv0(\bmod 4)\end{cases}$,即 v_0,u_0 均为偶然,故有 $\left(\frac{v_0}{2}\right)^2+13\left(\frac{\mu_0}{2}\right)^2=4$,即 $\left\{\frac{v_0}{2},\frac{\mu_0}{2}\right\}$ 是式(1)的本原解.

若 $k=9$,由 $k=3$ 的情形知 $3\mid d$. 令 $d=3i=(v_0,u_0)\geqslant 3$,由式(9)得 $i^2\mid n$. 再由式(8),得 $S_1\left(\frac{u_0}{i}\right)\equiv\left(\frac{v_0}{i}\right)\left(\bmod \frac{n}{i}\right)$.

因而 $\frac{9n}{i^2}=\left(\frac{v_0}{i^2}\right)^2+13\left(\frac{u_0}{i^2}\right)^2\equiv S_1^2\left(\frac{u_0}{i}\right)^2+13\left(\frac{u_0}{i^2}\right)^2\equiv0\left(\bmod \frac{n}{i}\right)$,这里用到了 $S_1^2\equiv-13\left(\bmod \frac{n}{i}\right)$,且仅当 $i=1$ 或 $i=3$ 或 $i=9$ 时成立. 但 $i=3$ 和 $i=9$ 时,$S_1^2\equiv-13(\bmod n)$ 无解,矛盾. 故 $i=1$,而从 $\left\{\frac{v_0}{3},\frac{u_0}{3}\right\}$ 是式(1)的本原解.

若 $k=10$,即 $v_0^2+13u_0^2=10n$,则 $v_0^2+13u_0^2\equiv v_0^2+3u_0^2\equiv0(\bmod 5)$,故有

$$\begin{cases}v_0^2\equiv0(\bmod 5)\\u_0^2\equiv0(\bmod 5)\end{cases}\text{或}\begin{cases}v_0^2\equiv1(\bmod 5)\\u_0^2\equiv3(\bmod 5)\end{cases}\text{或}\begin{cases}v_0^2\equiv2(\bmod 5)\\u_0^2\equiv1(\bmod 5)\end{cases}\text{或}\begin{cases}v_0^2\equiv3(\bmod 5)\\u_0^2\equiv4(\bmod 5)\end{cases}\text{或}\begin{cases}v_0^2\equiv4(\bmod 5)\\u_0^2\equiv2(\bmod 5)\end{cases}$$

但 $S^2\equiv2(\bmod 5)$ 和 $S^2\equiv3(\bmod 5)$ 无解,故 $\begin{cases}v_0\equiv0(\bmod 5)\\u_0\equiv0(\bmod 5)\end{cases}$,即 $5\mid d,d=(v_0,u_0)$,从而 $5\mid n$. 但这与 ${S_1}^2\equiv-13(\bmod n)$ 有解矛盾,故 $k\neq10$.

若 $k=12$ 成立,由 $k=3$ 的情形知 $3\mid d$. 这与 ${S_1}^2\equiv-13(\bmod n)$ 有解矛盾,故 $k\neq12$.

若 $k=13$ 成立,$v_0^2+13u_0^2=13n$,则 $13\mid v_0$. 令 $v_0=13w_0$ 代入式(9),得 $u_0^2+13w_0^2=n$. 由式(8),得 $S_1w_0\equiv-u_0(\bmod n)$. 仿上讨论,即得 $\{-u_0,v_0\}$ 是式(1)的本原解. 在式(6)中,当 x_1,y_1 同号时,取 $x_0=|x_1|,y_0=|y_1|$;当 x_1,y_1 异号时,取 $x_0=|x_1|,y_0=|y_1|$,重取 S_1 为 $-S_1$,则 $\{x_0,y_0\}$ 是式(1)的非负本原解,且满足式(6). 显然,同余方程(2)的解 $\pm S_1(\bmod n)$ 对应不定方程(1)的同一组非负本原解 $\{x_0,y_0\}$. 引理 3 证毕.

若 $\{x_1,y_1\},\{x_2,y_2\}$ 是式(1)的两组不同的非负本原解,满足

$$S_1y_1\equiv x_1(\bmod n),S_2y_2\equiv x_2(\bmod n)$$

则 $S_2\pm S_1$ 不同余.

如果 $S_2\equiv S_1(\bmod n)$,则 $S_1y_1x_2\equiv S_2y_2x_1(\bmod n)$,于是 $y_1y_2\equiv y_2x_1(\bmod n)$. 因 $1\leqslant x_i<\sqrt{n},1\leqslant y_i<\sqrt{\frac{n}{13}}$,故 $1\leqslant y_1x_2,y_2x_1<\frac{n}{\sqrt{2}}$,于是 $y_1x_2=y_2x_1$.

由 $(x_1,y_1)=(x_2,y_2)=1$,即得 $x_1=x_2,y_1=y_2$,矛盾.

如果 $S_2\equiv-S_1(\bmod n)$,则 $-S_1^2y_1y_2\equiv x_1x_2(\bmod n)$,即 $13y_1y_2\equiv x_1x_2(\bmod n)$.

因 $1\leqslant13y_1y_2,x_1x_2<n$,故 $13y_1y_2=x_1x_2$,于是 $13\mid x_1x_2$. 但 $(x_1,13)=1,(x_2,13)=1$,故 $(x_1x_2,13)=1$,矛盾.

由此可得,若 $\{x_0,y_0\}$ 为式(1)的一组非负本原解,则对应着式(2)的一对解 $\pm S_1(\bmod n)$. 反之,若 $\pm S_1(\bmod n)$ 为式(2)的一对解,则对应着式(1)的一组非负本原解 $\{x_0,y_0\}$. 所以式(1)的非负本原解数是式(2)的解数的一半.

定理 1 不定方程(1)的非负本原解数是

$$\frac{1}{2}\prod_{p\mid n}\left[1+\left(\frac{-13}{p}\right)\right]$$

由于 $n \in Z^+$,$n>13$ 并且$(n,13)=1$,因此式(1)的非负本原解必为正解,于是有推论1.

推论1 不定方程(1)的本原解数是其非负本原解数的4倍,即是

$$2\prod_{p|n}\left[1+\left(\frac{-13}{p}\right)\right]$$

下面来考察不定方程

$$x^2+13y^2=n^3 \tag{10}$$

$$a^2+13b^2=n \tag{11}$$

其中 $n \in Z^+$,$(n,13)=1$.

若$\{a,b\}$为式(11)的本原解,则 $n^3=(a^2+13b^2)^3=a^6+3\times 13a^4b^2+3\times 13^2a^2b^4+13^3b^6$. 配方得 $n^3=(a^3-39ab^2)^2+13(3a^2b-13b^3)^2$.

因为$(a,b)=1$,必有$(a,2b)=1$,故$(a^3-39ab^2,3a^2b-13b^3)=1$,于是式(10)有一组本原解$\{a^3-39ab^2,3a^2b-13b^3\}$. 令式(10)和(11)的本原解之集分别为 S 和 T,在 S 和 T 之间建立映射 f 如下:

$$f:S\to T$$

$$\{a,b\}\to\{a^3-39ab^2,3a^2b-13b^3\}$$

则称 f 是单射. 令

$$\begin{cases}x_0=a_1{}^3-39a_1b_1^2=a_2^3-39a_2b_2^2\\ y_0=3a_1{}^2b_1-13b_1{}^3=3a_2{}^2b_2-13b_2^3\end{cases}$$

这时$\{a_1,b_1\}$,$\{a_2,b_2\}\in S$,故$\{x_0,y_0\}\in T$,于是方程

$$x_0=a^3-39ab^2=a^3-3a(n-a^2)=4a^3-3na$$

即

$$a^3-\frac{3n}{4}a-\frac{x_0}{4}=0 \tag{12}$$

有两个有理根 a_1 和 a_2. 但式(12)的判别式

$$-4\left(-\frac{3n}{4}\right)^3-27\left(-\frac{x_0}{4}\right)^2=\frac{27}{16}(n^3-x_0^2)=\frac{54}{16}y_0^2=6\left(\frac{3y_0}{4}\right)^2$$

不是一个有理数的平方,故式(12)至多有一个有理根,于是 $a_1=a_2$. 由式(12)有$|b_1|=|b_2|$. 再由 y_0 的表达式,必有 $b_1=b_2$,所以 f 是单射. 由推论1,$|S|=|T|<\infty$,故 f 又是满射,从而 f 为双射,因此有定理2.

定理2 不定方程(10)的本原解为 $x=a^3-39ab^2$,$y=3a^2b-13b^3$,其中$\{a,b\}$为式(11)的本原解,$(a,2b)=1$.

显然,$n=1$ 时,式(10)和(11)的解均为$\{\pm 1,0\}$,仍可归结为表达式(12).

推论2 不定方程 $x^2+13y^2=z^3$ 的本原解为

$$x=a^3-39ab^2,y=3a^2b-13b^3,z=a^2+13b^2$$

这里$(a,2b)=1$.

定理3 不定方程 $y^2=x^3-13$ 仅有解 $x=17$,$y=\pm 70$.

证明 把 $y^2=x^3-13$ 改写为 $y^2+13\times 1^2=x^3$,显然$(x,y)=1$. 由推论(2),得

$$y=a^3-39ab^2,1=3a^2b-13b^3,x=a^2+13b^2$$

得 $a=\pm 2$,$b=-1$,故 $x=17$,$y=\pm 70$.

参考文献:

[1] 李伟. 不定方程 $y^3=x^2+2$ 的初等解法[J]. 四川大学学报:自然科学版,1997,34(1):16-19

[2] 潘承洞,潘承彪. 初等数论[M]. 北京:北京大学出版社,1992

Elementary Solution Method to Diophantine Equation $y^2 = x^3 - 13$

XIONG Jun[1], JING Yong[2]

(1. Chongqing Yucai Middle School, Chongqing 400050, China;

2. Department of Mathematics, Southwest University of Finance and Economics, Chengdu 610074, China)

Abstract: This paper discusses that the Diophantine equation $y^2 = x^3 - 13$ has the only elementary solution $x = 17$, $y = \pm 70$.

Key words: Diophantine equation; elementary solution; primitive solution

责任编辑:罗泽举
校　　对:李翠薇

(上接第 16 页)

Strong Convergence Theorems for a Common Zero Point of an Infinite Family of Strongly Monotone Mappings

TANG Yan

(College of Mathematics and Statistics, Chongqing Technology and Business University, Chongqing 400067, China)

Abstract: In this paper, arbitrary non-empty bounded closed convex subset having properties of fixed point of nonexpansive mappings is assumed in a real Banach space of differential norm with consistent Gâteaux. The strong convergence theorem for iterative scheme of a common zero point of an infinite family of strong monotone mappings is discussed and is proved under some suitable conditions.

Key words: monotone mappings; fixed point; zero point; strong convergence

责任编辑:李翠薇