DOI:10.11721/cqnuj20160504

椭圆曲线 $y^2=x^3+27x+62$ 的整数点*

过　静
(江西科技师范大学 数学与计算机科学学院,南昌 330013)

摘要:椭圆曲线的整数点是数论中的一个重要问题。关于椭圆曲线 $y^2=x^3+27x+62$ 的整数点问题至今仍未解决。利用同余、Legendre 符号的性质等初等方法证明了椭圆曲线 $y^2=x^3+27x+62$ 无正整数点,从而推进了该类椭圆曲线的研究。

关键词:椭圆曲线;正整数点;同余;Legendre 符号
中图分类号:O156.1　　**文献标志码**:A　　**文章编号**:1672-6693(2016)05-0050-04

椭圆曲线的整数点是数论和算术代数几何学中基本而又重要的问题,关于椭圆曲线

$$y^2=x^3+27x-62 \tag{1}$$

的整数点问题,目前已有如下结论:1987 年,Zagier[1] 提出了椭圆曲线(1)的整数点的问题,该问题对于讨论椭圆曲线的算术性质有重要的意义;2009 年,祝辉林等人[2] 运用代数数论和 p-adic 分析方法找出了椭圆曲线(1)的全部整数点;2010 年,吴华明[3] 运用初等数论方法给出了椭圆曲线(1)的全部整数点;同年,贺艳峰[4] 在博士论文中同样运用初等数论方法给出了椭圆曲线(1)的全部整数点。而对于椭圆曲线 $y^2=x^3+27x+62$ 的整数点问题,目前还没有相关结论。本文得出了如下结论。

定理　椭圆曲线

$$y^2=x^3+27x+62 \tag{2}$$

无正整数点。

1 相关引理

引理 1[5]　设 $a>1,(a,b)\in\mathbf{N}^2$,ab 不是完全平方数,如果 $ax^2-by^2=1$ 有解 $(x,y)\in\mathbf{N}^2$,设 $x_1\sqrt{a}+y_1\sqrt{b}$ 是方程 $ax^2-by^2=1(x,y\in\mathbf{Z})$ 的基本解,则 $ax^2-by^2=1$ 的任一组解可以表示为:$x\sqrt{a}+y\sqrt{b}=\pm(x_1\sqrt{a}+y_1\sqrt{b})^{2n+1}$,$n\in\mathbf{Z}$。

引理 2[6]　设 D 是一个非平方的正整数,则方程 $x^2-Dy^4=1$ 至多有 2 组正整数解 (x,y)。如果 $x^2-Dy^4=1$ 恰有两组正整数解,则当 $D=2^{4s}\times 1\ 785$,其中 $s\in\{0,1\}$ 时,$(x_1,y_1)=(169,2^{1-s})$ 且 $(x_2,y_2)=(6\ 525\ 617\ 281,2^{1-s}\times 6\ 214)$;当 $D\neq 2^{4s}\times 1\ 785$ 时,$(x_1,y_1)=(u_1,\sqrt{v_1})$ 且 $(x_2,y_2)=(u_2,\sqrt{v_2})$,这里 (u_n,v_n) 是 Pell 方程 $U^2-DV^2=1$ 的正整数解。如果方程 $x^2-Dy^4=1$ 仅有 1 组正整数解 (x,y) 且正整数 n 适合 $(x,y^2)=(u_n,v_n)$,则当 n 是偶数时,必有 $n=2$;当 n 是奇数时,必有 $n=1$ 或 p,这里 p 是适合 $p\equiv 3\pmod 4$ 的素数。

2 定理证明

证明　设 (x,y) 是椭圆曲线(2)的整数点,则由(2)式得

$$y^2=(x+2)(x^2-2x+31)。 \tag{3}$$

因为 $\gcd(x+2,x^2-2x+31)=\gcd(x+2,(x+2)^2-6(x+2)+39)=\gcd(x+2,39)=1$ 或 3 或 13 或 39,故(3)式可分解为:

* **收稿日期**:2015-11-25　**修回日期**:2015-12-21　**网络出版时间**:2016-07-13 14:05
资助项目:江西省资源共享课程资助项目;江西科技师范大学校级重点课题(No. 2015xjzd002)
作者简介:过静,女,副教授,研究方向为初等数论、代数,E-mail:651077099@qq.com
网络出版地址:http://www.cnki.net/kcms/detail/50.1165.N.20160713.1405.056.html

情形Ⅰ，$x+2=u^2$，$x^2-2x+31=v^2$，$y=\pm uv$，$\gcd(u,v)=1$；

情形Ⅱ，$x+2=3u^2$，$x^2-2x+31=3v^2$，$y=\pm 3uv$，$\gcd(u,v)=1$；

情形Ⅲ，$x+2=13u^2$，$x^2-2x+31=13v^2$，$y=\pm 13uv$，$\gcd(u,v)=1$；

情形Ⅳ，$x+2=39u^2$，$x^2-2x+31=39v^2$，$y=\pm 39uv$，$\gcd(u,v)=1$。

对情形Ⅰ，因为 $u^2\equiv 0,1 \pmod 4$，故 $x=u^2-2\equiv 2,3 \pmod 4$，因此 $x^2-2x+31\equiv 2,3 \pmod 4$，而 $v^2\equiv 0,1 \pmod 4$，故有 $2,3 \pmod 8\equiv x^2-2x+31=v^2\equiv 0,1 \pmod 4$，矛盾，故情形Ⅰ不成立。

对情形Ⅱ，因为 $u^2\equiv 0,1,4 \pmod 8$，故 $x=3u^2-2\equiv 1,2,6 \pmod 8$，因此 $x^2-2x+31\equiv 6,7 \pmod 8$，而 $v^2\equiv 0,1,4 \pmod 8$，则 $3v^2\equiv 0,3,4 \pmod 8$，故有 $6,7 \pmod 8\equiv x^2-2x+31=3v^2\equiv 0,3,4 \pmod 8$，矛盾，故情形Ⅱ不成立。

对情形Ⅲ，因为 $u^2\equiv 0,1 \pmod 4$，故 $x=13u^2-2\equiv 2,3 \pmod 4$，因此 $x^2-2x+31\equiv 2,3 \pmod 4$，而 $v^2\equiv 0,1 \pmod 4$，则 $13v^2\equiv 0,1 \pmod 4$，故有 $2,3 \pmod 4\equiv x^2-2x+31=13v^2\equiv 0,1 \pmod 4$，矛盾，故情形Ⅲ不成立。

对情形Ⅳ，当 $2\nmid u$ 时有 $u^2\equiv 1 \pmod 4$，故有 $x=39u^2-2\equiv 1 \pmod 4$，因此 $x^2-2x+31\equiv 2 \pmod 4$，而 $v^2\equiv 0,1 \pmod 4$，则 $39v^2\equiv 0,3 \pmod 4$，故有 $2 \pmod 4\equiv x^2-2x+31=39v^2\equiv 0,3 \pmod 4$，矛盾，因此 $2\nmid u$ 不成立，所以 $2\mid u$。令 $u=2w$，$w\in\mathbf{Z}$，则 $x+2=39u^2$ 为 $x+2=156w^2$，将 $x+2=156w^2$ 代入 $x^2-2x+31=39v^2$ 得，$(12w^2-1)^2+480w^4=v^2$，即

$$(v+12w^2-1)(v-12w^2+1)=480w^4。\tag{4}$$

又 $\gcd(v+12w^2-1,v-12w^2+1)=\gcd(24w^2-2,v-12w^2+1)=\gcd(2(12w^2-1),\ v-(12w^2-1))$。因为 $2\mid u$，故由 $x+2=39u^2$ 知 $2\mid x$，则由 $x^2-2x+31=39v^2$ 得 $2\nmid v$，故 $2\mid[v-(12w^2-1)]$。又 $\gcd(2(12w^2-1),v-(12w^2-1))=2\gcd(12w^2-1,v-(12w^2-1))=2\gcd(12w^2-1,v)$。设 $\gcd(12w^2-1,v)=d$，则 $d\mid v$，$d\mid(12w^2-1)$，故由(4)式知 $d\mid 480w^4$。又 $\gcd(12w^2-1,480w^4)=\gcd(12w^2-1,40w^2(12w^2-1)+40w^2)=\gcd(12w^2-1,40w^2)=\gcd(12w^2-1,3(12w^2-1)+4w^2+3)=\gcd(12w^2-1,4w^2+3)=\gcd(3\cdot(4w^2+3)-10,4w^2+3)=\gcd(10,4w^2+3)=1$ 或 5。若 $\gcd(12w^2-1,480w^4)=5$，则有 $12w^2-1\equiv 0 \pmod 5$，即 $12w^2\equiv 1 \pmod 5$，而 Legendre 符号值 $\left(\frac{12w^2}{5}\right)=\left(\frac{3}{5}\right)\cdot\left(\frac{(2w)^2}{5}\right)=-1$，故 $12w^2\equiv 1 \pmod 5$ 不成立，则 $\gcd(12w^2-1,480w^4)=1$，因此 $d=1$，即 $\gcd(12w^2-1,v)=1$，所以 $\gcd(v+12w^2-1,v-12w^2+1)=2$。又 $480=2^5\times 3\times 5$，故(4)式可分解为：

$$v+12w^2-1=2sa^4,v-12w^2+1=\frac{240}{s}b^4,w=ab,\gcd(a,b)=1,\gcd\left(s,\frac{120}{s}\right)=1,$$

$$s=1,3,5,3\times 5,2^3,2^3\times 3,2^3\times 5,2^3\times 3\times 5。\tag{5}$$

由(5)式的前两式，得

$$12w^2-1=sa^4-\frac{120}{s}b^4。\tag{6}$$

对(6)式两边取模 3，得

$$-1\equiv sa^4-\frac{120}{s}b^4 \pmod 3。\tag{7}$$

对(6)式两边取模 4，得

$$-1\equiv sa^4-\frac{120}{s}b^4 \pmod 4。\tag{8}$$

当 $s=1$ 时，(7)式为

$$-1\equiv a^4 \pmod 3。\tag{9}$$

因为 Legendre 符号值 $\left(\frac{-1}{3}\right)=-1$，Legendre 符号值 $\left(\frac{a^4}{3}\right)=\left(\frac{(a^2)^2}{3}\right)=1$，故 $s=1$ 时，Legendre 符号值 $\left(\frac{a^4}{3}\right)=1$，故(9)式不成立，因此 $s=1$ 时(4)式不成立，即情形Ⅳ不成立。

当 $s=3\times 5,2^3\times 3$ 时，(7)式为

$$1\equiv\frac{120}{s}b^4 \pmod 3。\tag{10}$$

因为 Legendre 符号值$\left(\frac{1}{3}\right)=1$，Legendre 符号值$\left(\frac{b^4}{3}\right)=\left(\frac{(b^2)^2}{3}\right)=1$，故 Legendre 符号值$\left(\frac{\frac{120}{s}b^4}{3}\right)=\left(\frac{\frac{120}{s}}{3}\right)\left(\frac{b^4}{3}\right)=\left(\frac{\frac{120}{s}}{3}\right)$。故 $s=3\times5$ 时，Legendre 符号值$\left(\frac{\frac{120}{s}b^4}{3}\right)=\left(\frac{8}{3}\right)=\left(\frac{2}{3}\right)=-1$；$s=2^3\times3$ 时，Legendre 符号值$\left(\frac{\frac{120}{s}b^4}{3}\right)=\left(\frac{5}{3}\right)=\left(\frac{2}{3}\right)=-1$，故 $s=3\times5,2^3\times3$ 时(10)式不成立，因此 $s=3\times5,2^3\times3$ 时(4)式不成立，即情形Ⅳ不成立。

当 $s=5$ 时，(8)式为

$$-1\equiv sa^4\pmod 4。\tag{11}$$

因为 $a^2\equiv0,1\pmod 4$，故 $sa^4=5a^4\equiv0,1\pmod 4$，则(11)式为$-1\equiv5a^4\equiv0,1\pmod 4$，矛盾，故(11)式不成立，因此 $s=5$ 时(4)式不成立，即情形Ⅳ不成立。

当 $s=2^3,2^3\times5$ 时，(8)式为

$$1\equiv\frac{120}{s}b^4\pmod 4。\tag{12}$$

因为 $b^2\equiv0,1\pmod 4$，故 $s=2^3$ 时$\frac{120}{s}b^4=15b^4\equiv0,3\pmod 4$，而 $s=2^3\times5$ 时，$\frac{120}{s}b^4=3b^4\equiv0,3\pmod 4$，则 $s=2^3,2^3\times5$ 时，(12)式为 $1\equiv0,3\pmod 4$，矛盾，故(12)式不成立，因此 $s=2^3,2^3\times3\times5$ 时，(4)式不成立，即情形Ⅳ不成立。

当 $s=3$ 时，(6)式为 $12w^2-1=3a^4-40b^4$，将(5)式的 $w=ab$ 代入得 $12a^2b^2-1=3a^4-40b^4$，配方得

$$52b^4-3(a^2-2b^2)^2=1。\tag{13}$$

令 $r=2b^2,t=a^2-2b^2,r,t\in\mathbf{N}$，则(13)式为

$$13r^2-3t^2=1,\tag{14}$$

又(1,2)为方程(14)的基本解，则由引理1知方程(14)的一切整数解可表为：$r\sqrt{13}+t\sqrt{3}=\pm(\sqrt{13}+2\sqrt{3})^{2n+1}$，$n\in\mathbf{Z}$，由此得方程(13)的一切正整数解$(2b^2,a^2-2b^2)$满足：

$$2b^2\sqrt{13}+(a^2-2b^2)\sqrt{3}=(\sqrt{13}+2\sqrt{3})^{2n+1},n\in\mathbf{N}。\tag{15}$$

由(15)式得，$2b^2=\sum_{i=0}^{n}\binom{2n+1}{2i}\times\sqrt{13}^{2(n-i)}\times2^{2i}\times\sqrt{3}^{2i}=\sum_{i=0}^{n}\binom{2n+1}{2i}\times13^{n-i}\times12^i=13^n+\sum_{i=1}^{n}\binom{2n+1}{2i}\times13^{n-i}\times3^i\times4^i$，即

$$2b^2=13^n+\sum_{i=1}^{n}\binom{2n+1}{2i}\times13^{n-i}\times3^i\times4^i。\tag{16}$$

因为 $\sum_{i=1}^{n}\binom{2n+1}{2i}\times13^{n-i}\times3^i\times4^i$ 为偶数，则 $13^n+\sum_{i=1}^{n}\binom{2n+1}{2i}\times13^{n-i}\times3^i\times4^i$ 为奇数，故(16)式不成立，所以方程(14)无整数解，因此方程(13)无整数解，故 $s=3$ 时，(4)式不成立，即情形Ⅳ不成立。

当 $s=2^3\times3\times5$ 时，(6)式为 $12w^2-1=120a^4-b^4$，将(5)式的 $w=ab$ 代入得，$12a^2b^2-1=120a^4-b^4$，配方得

$$(6a^2+b^2)^2-156a^4=1。\tag{17}$$

令 $p=6a^2+b^2$，则(17)式为

$$p^2-156a^4=1。\tag{18}$$

令 $q=2a^2,p,q\in\mathbf{N}$，则(18)式为

$$p^2-39q^2=1。\tag{19}$$

由引理2得方程(18)至多有一组正整数解(p,a)，且若方程(18)有正整数解(p,a)，则方程(19)有正整数解$(p,q)=(p,2a^2)$。又因为 Pell 方程(19)的基本解为(25,4)，则方程(19)的全部正整数解可表为 $p_n+q_n\sqrt{39}=$

$(25+4\sqrt{39})^n, n\in\mathbf{Z}^+$。

由此可知方程(17)的整数解满足：

$$(6a^2+b^2)+a^2\sqrt{156}=(6a^2+b^2)+2a^2\sqrt{39}=(25+4\sqrt{39})^n, n\in\mathbf{Z}^+, \tag{20}$$

则由引理 2 知 $n=2$ 或 $2\nmid n$。

由(20)式，得：

$$2a^2=\begin{cases}\sum\limits_{i=0}^{\frac{n-1}{2}}\binom{n}{2i+1}\times 25^{n-2i-1}\times 4^{2i+1}\times 39^i, & 2\nmid n,\\ \sum\limits_{i=0}^{\frac{n}{2}}\binom{n}{2i+1}\times 25^{n-2i-1}\times 4^{2i+1}\times 39^i, & 2\mid n。\end{cases}$$

则有：

$$2a^2=\begin{cases}4\left(25^{n-1}+\sum\limits_{i=1}^{\frac{n-1}{2}}\binom{n}{2i+1}\times 25^{n-2i-1}\times 4^{2i}\times 39^i\right), & 2\nmid n,\\ 4\left(25^{n-1}+\sum\limits_{i=1}^{\frac{n}{2}}\binom{n}{2i+1}\times 25^{n-2i-1}\times 4^{2i}\times 39^i\right), & 2\mid n。\end{cases} \tag{21}$$

由(21)式可得 $2a^2\equiv 4\pmod 8$，即有 $a^2\equiv 2\pmod 8$，显然不成立，故方程(18)无正整数解，因此方程(18)仅有平凡解$(p,a)=(1,0)$。由 $p=6a^2+b^2=1$，得 $a=0, b=\pm 1$，此时得出椭圆曲线(2)有整数点$(x,y)=(-2,0)$。故 $s=2^3\times 3\times 5$ 时得出椭圆曲线(2)有整数点$(x,y)=(-2,0)$。

综上有情形Ⅳ下椭圆曲线(2)仅有整数点$(x,y)=(-2,0)$，故情形Ⅳ下椭圆曲线(2)无正整数点。综上所述定理得证。 证毕

参考文献：

[1] Zagier D. Lager integral point on elliptic curves [J]. Math Comp, 1987, 48: 425-436.

[2] Zhu H L, Chen J H. Integral point on $y^2=x^3+27x-62$ [J]. J Math Study, 2009, 42(2): 117-125.

[3] 吴华明. 椭圆曲线 $y^2=x^3+27x-62$ 的整数点[J]. 数学学报中文版, 2010, 53(1): 205-208.
Wu H M. Points on the elliptic curves $y^2=x^3+27x-62$ [J]. J Acta Mathematica Sinica, 2010, 53(1): 205-208.

[4] 贺艳峰. 数论函数的均值分布及整点问题的研究[D]. 西安：西北大学, 2010.
He Y F. Mean value formula and integer point problem for some number theory functions[D]. Xi'an: Northwest University, 2010.

[5] 夏圣亭. 不定方程浅说[M]. 天津：天津人民出版社, 1980.
Xia S T. On the Diopantine equation[M]. Tianjin: Tianjin People Press, 1980.

[6] Togbé A, Voutier P M, Walsh P G. Solving a family of the equations with an application to the equation $x^2-Dy^4=1$ [J]. Acta Arith, 2005, 120(1): 39-58.

The Integral Points on the Elliptic Curve $y^2=x^3+27x+62$

GUO Jing

(College of Mathematics and Computer Science, Jiangxi Science and Technology Normal University, Nanchang 330013, China)

Abstract: The integral points on elliptic curve are a very important problem of number theory. The integral points on the elliptic curve $y^2=x^3+27x+62$ still remain unresolved. Using some properties of the solutions to congruence and Legendre symbol, it was proved that the elliptic curve $y^2=x^3+27x+62$ has no positive integer points. These results promote the kind of elliptic curve.

Key words: elliptic curve; integer point; congruence; Legendre symbol

(责任编辑 游中胜)