DOI: 10.13718/j.cnki.xdzk.2017.06.011

椭圆曲线 $y^2=(x+2)(x^2-2x+p)$ 的整数点①

杜先存[1]，　赵建红[2]，　万　飞[1]

1. 红河学院 教师教育学院，云南 蒙自 661199；2. 丽江师范高等专科学校 数学与计算机科学系，云南 丽江 674199

摘要：利用 Legendre 符号、同余式、Pell 方程的解的性质等初等方法证明了：当 $p=36s^2-5(s\in\mathbb{Z}_+,\ 2\nmid s)$，而 $6s^2-1, 12s^2+1$ 均为素数时，椭圆曲线 $y^2=(x+2)(x^2-2x+p)$ 仅有整数点为 $(x,y)=(-2,0)$.

关　键　词：椭圆曲线；整数点；Pell 方程；Legendre 符号；同余

中图分类号：O156.2　　**文献标志码**：A　　**文章编号**：1673-9868(2017)06-0069-05

3 次不定方程是一类基本而又重要的方程，目前关于 3 次不定方程的结论已经比较多[1-2]. 而椭圆曲线 $y^2=(x+a)(x^2-ax+p)$ $(a,p\in\mathbb{Z})$ 是 3 次不定方程中的一类特殊的方程. 椭圆曲线的整数点问题是数论和算术代数几何学中基本而又重要的问题，其结果有着广泛的应用. 近年来，寻找椭圆曲线的整数点问题引起了人们的兴趣. 关于椭圆曲线的整数点问题，目前已有一些结论. 当 $a=-2$ 时，椭圆曲线的结论见文献[3-7]；当 $a=2$ 时，椭圆曲线的结果仅限于 $p=31$ 的情况，见文献[8]. 本文将对 $a=2$，$p=36s^2-5(s\in\mathbb{Z}_+,\ 2\nmid s)$ 时椭圆曲线的整数点问题进行研究.

定理 1　设 $p=36s^2-5(s\in\mathbb{Z}_+,\ 2\nmid s)$，而 $6s^2-1$，$12s^2+1$ 均为素数，则椭圆曲线

$$y^2=(x+2)(x^2-2x+p) \tag{1}$$

仅有整数点为 $(x,y)=(-2,0)$.

证　设 (x,y) 是椭圆曲线(1)的整数点. 因为 $12s^2+1$ 为素数，所以

$$\gcd(x+2,\ x^2-2x+p)=\gcd(x+2,\ p+8)=\gcd(x+2,\ 3(12s^2+1))=1,3,12s^2+1,\ 3(12s^2+1)$$

设 $t=12s^2+1$，故椭圆曲线(1)可分解为以下 4 种可能的情形：

情形 Ⅰ　$x+2=u^2$，$x^2-2x+p=v^2$，$y=uv$，$\gcd(u,v)=1(u,v\in\mathbb{Z})$；

情形 Ⅱ　$x+2=3u^2$，$x^2-2x+p=3v^2$，$y=3uv$，$\gcd(u,v)=1(u,v\in\mathbb{Z})$；

情形 Ⅲ　$x+2=tu^2$，$x^2-2x+p=tv^2$，$y=tuv$，$\gcd(u,v)=1(u,v\in\mathbb{Z})$；

情形 Ⅳ　$x+2=3tu^2$，$x^2-2x+p=3tv^2$，$y=3tuv$，$\gcd(u,v)=1(u,v\in\mathbb{Z})$.

下面分别讨论这 4 种情形下椭圆曲线(1)的整数点的情况.

情形 Ⅰ　因为 $p=36s^2-5$，故 $p\equiv-1\pmod 4$. 又因 $x=u^2-2\equiv 2,3\pmod 4$，因此 $x^2-2x+p\equiv$

① 收稿日期：2016-05-24

基金项目：云南省科技厅应用基础研究计划青年项目(2013FD060)；云南省教育厅科研基金(2014Y462)；红河学院校级课题(XJ15Y22)；红河学院中青年学术骨干培养资助项目(2015GG0207)；喀什大学校级课题((14)2507)；江西省教育厅科学技术研究项目(GJJ160782).

作者简介：杜先存(1981-)，女，云南凤庆人，副教授，主要从事初等数论的研究.

通信作者：万　飞，副教授.

$2,3(\mathrm{mod}\ 4)$，故有

$$2,3(\mathrm{mod}\ 4)\equiv x^2-2x+p=v^2\equiv 0,1(\mathrm{mod}\ 4)$$

显然矛盾，故该情形下椭圆曲线(1)无整数点.

情形Ⅱ 因为 $p=36s^2-5$，$2\nmid s$，故 $p\equiv -1(\mathrm{mod}\ 8)$. 又因 $x=3u^2-2\equiv 1,2,6(\mathrm{mod}\ 8)$，则 $x^2-2x+p\equiv 6,7(\mathrm{mod}\ 8)$，故有

$$6,7(\mathrm{mod}\ 8)\equiv x^2-2x+p=3v^2\equiv 0,3,4(\mathrm{mod}\ 8)$$

显然矛盾，故该情形下椭圆曲线(1)无整数点.

情形Ⅲ 因为 $p=36s^2-5$，故 $p\equiv -1(\mathrm{mod}\ 4)$. 又因 $x=13u^2-2\equiv 2,3(\mathrm{mod}\ 4)$，因此 $x^2-2x+p\equiv 2,3(\mathrm{mod}\ 4)$. 因 $t=12s^2+1\equiv 1(\mathrm{mod}\ 4)$，故 $tv^2\equiv 0,1(\mathrm{mod}\ 4)$，故有

$$2,3(\mathrm{mod}\ 4)\equiv x^2-2x+p=tv^2\equiv 0,1(\mathrm{mod}\ 4)$$

显然矛盾，故该情形下椭圆曲线(1)无整数点.

情形Ⅳ 当 $2\nmid u$ 时，有 $u^2\equiv 1(\mathrm{mod}\ 4)$. 因为 $t=12s^2+1\equiv 1(\mathrm{mod}\ 4)$，因此 $x=3tu^2-2\equiv 1(\mathrm{mod}\ 4)$. 又因 $p=36s^2-5$，故 $p\equiv -1(\mathrm{mod}\ 4)$，因此 $x^2-2x+p\equiv 2(\mathrm{mod}\ 4)$. 而 $3tv^2\equiv 0,3(\mathrm{mod}\ 4)$，故有

$$2(\mathrm{mod}\ 4)\equiv x^2-2x+p=3tv^2\equiv 0,3(\mathrm{mod}\ 4)$$

矛盾，因此 $2\nmid u$ 不成立，所以 $2\mid u$. 令 $u=2m(m\in\mathbb{Z})$，则 $x+2=3tu^2$ 为 $x+2=12tm^2$，代入 $x^2-2x+p=3tv^2$ 得 $(12tm^2-3)^2+p-1=3tv^2$. 又因为 $p=36s^2-5$，$t=12s^2+1$，所以 $p=3t-8$，代入 $(12tm^2-3)^2+p-1=3tv^2$，配方得 $(12m^2-1)^2+48(t-3)m^4=v^2$，即

$$(v+12m^2-1)(v-12m^2+1)=48(t-3)m^4 \tag{2}$$

因为 $2\mid u$，故由 $x+2=3tu^2$ 知 $2\mid x$，则由 $x^2-2x+p=3tv^2$ 得 $2\nmid v$，故 $2\mid[v-(12m^2-1)]$. 因此

$$\gcd(v+12m^2-1,\ v-12m^2+1)=2\gcd(12m^2-1,\ v)$$

设 $\gcd(12m^2-1,\ v)=d$，则由(2)式知 $d\mid 48(t-3)m^4$. 又因 $6s^2-1$ 为素数，则

$$\begin{aligned}\gcd(12m^2-1,\ 48(t-3)m^4)&=\gcd(12m^2-1,\ 4(12s^2-2)m^2)=\\&\gcd(6s^2-1,\ 2m^2-s^2)=\\&1,6s^2-1\end{aligned}$$

若 $\gcd(12m^2-1,\ 48(t-3)m^4)=6s^2-1$，则有 $12m^2-1\equiv 0(\mathrm{mod}\ (6s^2-1))$，即 $12m^2\equiv 1(\mathrm{mod}\ (6s^2-1))$. 因 Legendre 符号值 $\left(\frac{12m^2}{6s^2-1}\right)=\left(\frac{3}{6s^2-1}\right)=\left(\frac{6s^2-1}{3}\right)=-1$，故 $12m^2\equiv 1(\mathrm{mod}\ (6s^2+1))$ 不成立，则 $\gcd(12m^2-1,\ 48(t-3)m^2)=1$，因此 $d=1$，即 $\gcd(12m^2-1,\ v)=1$. 所以

$$\gcd(v+12m^2-1,\ v-12m^2+1)=2$$

因为 $48(t-3)=96(6s^2-1)$，而 $6s^2-1$ 为素数，故(2)式可分解为：

$$\begin{cases}v+12m^2-1=2ra^4\\ v-12m^2+1=\dfrac{48(6s^2-1)}{r}b^4\end{cases} \tag{3}$$

其中 $m=ab$，$\gcd(a,\ b)=1$，$\gcd\left(r,\ \dfrac{24(6s^2-1)}{r}\right)=1$，$a,b\in\mathbb{Z}$，且

$$r=1,2^3,3,2^3\times 3\times(6s^2-1),2^3\times(6s^2-1),6s^2-1,2^3\times 3,3\times(6s^2-1)$$

由(3)式得

$$12m^2-1=ra^4-\frac{24(6s^2-1)}{r}b^4 \tag{4}$$

对(4)式两边取模4，得

$$-1\equiv ra^4-\frac{24(6s^2-1)}{r}b^4(\mathrm{mod}\ 4) \tag{5}$$

对(4)式两边取模3，得

$$-1\equiv ra^4-\frac{24(6s^2-1)}{r}b^4\pmod 3 \tag{6}$$

当 $r=6s^2-1$ 时，(5) 式为

$$-1\equiv ra^4\pmod 4 \tag{7}$$

因为 $2\nmid s$，所以 $ra^4=(6s^2-1)a^4\equiv 0,1\pmod 4$，则(7) 式为 $-1\equiv ra^4\equiv 0,1\pmod 4$，显然矛盾，故(7) 式不成立，因此 $r=6s^2-1$ 时(3) 式不成立，即情形 Ⅳ 不成立.

当 $r=2^3,2^3\times(6s^2-1)$ 时，(5) 式为

$$1\equiv\frac{24(6s^2-1)}{r}b^4\pmod 4 \tag{8}$$

因为 $2\nmid s$，所以 $r=2^3$ 时，有

$$\frac{24(6s^2-1)}{r}b^4=3(6s^2-1)b^4\equiv 0,3\pmod 4$$

而 $r=2^3(6s^2-1)$ 时，有

$$\frac{24(6s^2-1)}{r}b^4=3b^4\equiv 0,3\pmod 4$$

故当 $r=2^3,2^3\times(6s^2-1)$ 时，(8) 式为 $1\equiv 0,3\pmod 4$，显然矛盾，故(8) 式不成立，因此当 $r=2^3,2^3\times(6s^2-1)$ 时(3) 式不成立，即情形 Ⅳ 不成立.

当 $r=1$ 时，(6) 式为

$$-1\equiv ra^4\pmod 3 \tag{9}$$

因为 $r=1$ 时，Legendre 符号值 $\left(\frac{ra^4}{3}\right)=\left(\frac{a^4}{3}\right)=1$，而 Legendre 符号值 $\left(\frac{-1}{3}\right)=-1$，故(9) 式不成立，因此当 $r=1$ 时(3) 式不成立，即情形 Ⅳ 不成立.

当 $r=3(6s^2-1),2^3\times 3$ 时，(6) 式为

$$1\equiv\frac{24(6s^2-1)}{r}b^4\pmod 3 \tag{10}$$

因为 Legendre 符号值 $\left(\frac{1}{3}\right)=1$，而 $r=3(6s^2-1)$ 时 Legendre 符号值 $\left(\frac{\frac{24(6s^2-1)}{r}b^4}{3}\right)=\left(\frac{8b^4}{3}\right)=-1$，故(10) 式不成立；$r=2^3\times 3$ 时，Legendre 符号值 $\left(\frac{\frac{24(6s^2-1)}{r}b^4}{3}\right)=\left(\frac{6s^2-1}{3}\right)=\left(\frac{-1}{3}\right)=-1$，故 $r=2^3\times 3$ 时(10) 式不成立. 因此 $r=3(6s^2-1),2^3\times 3$ 时(3) 式不成立，即情形 Ⅳ 不成立.

当 $r=2^3\times 3\times(6s^2-1)$ 时，(4) 式为 $12m^2-1=2^3\times 3\times(6s^2-1)a^4-b^4$. 将(3) 式的 $m=ab$ 代入并配方，得

$$(6a^2+b^2)^2-12(12s^2+1)a^4=1 \tag{11}$$

令 $w=6a^2+b^2$，则(11) 式为

$$w^2-12(12s^2+1)a^4=1 \tag{12}$$

由文献[9] 的定理 1 得，方程(12) 至多有 1 组正整数解 (w,a). 又由文献[7] 的引理 6 得，Pell 方程

$$w^2-12(12s^2+1)a^2=1$$

的基本解为 $(w_1,a_1)=(24s^2+1,2s)$，则方程(12) 的全部正整数解可表示为

$$w_n+a_n\sqrt{12(12s^2+1)}=w_n+2a_n\sqrt{3(12s^2+1)}=((24s^2+1)+4s\sqrt{3(12s^2+1)})^n\qquad n\in\mathbb{Z}_+$$

由此可知方程(11) 的正整数解满足

$$(6a^2+b^2)+2a^2\sqrt{3(12s^2+1)}=((24s^2+1)+4s\sqrt{3(12s^2+1)})^n\qquad n\in\mathbb{Z}_+ \tag{13}$$

由(13) 式有

$$2a^2=\begin{cases}4sn(24s^2+1)^{n-1}+\sum\limits_{i=1}^{\frac{n-1}{2}}\binom{n}{2i+1}\times(24s^2+1)^{n-2i-1}\times(4s)^{2i+1}\times3^i\times(12s^2+1)^i & 2\nmid n\\ \sum\limits_{i=1}^{\frac{n}{2}}\binom{n}{2i-1}\times(24s^2+1)^{n-2i+1}\times(4s)^{2i-1}\times3^{i-1}\times(12s^2+1)^{i-1} & 2\mid n\end{cases}\tag{14}$$

则由文献[7]的定理1得知 $n=2,2\nmid n$.

若 $2\nmid n$，因为 $2\nmid s$，故 $4ns\equiv4(\mathrm{mod}\ 8)$，$24s^2+1\equiv1(\mathrm{mod}\ 8)$.(14)式两边取模8，得 $a^2\equiv2(\mathrm{mod}\ 8)$，显然不成立，故方程(12)无正整数解，因此方程(11)仅有平凡解$(w,a)=(1,0)$.由 $w=6a^2+b^2=1$，得 $a=0$，$b=\pm1$，此时得出椭圆曲线(1)有整数点$(x,y)=(-2,0)$，故 $r=2^3\times3\times(6s^2-1)$ 时椭圆曲线(1)有整数点$(x,y)=(-2,0)$.

若 $n=2$，由(13)式得

$$6a^2+b^2=(24s^2+1)^2+(4s)^2[3(12s^2+1)]=$$
$$576s^4+48s^2+1+576s^4+48s^2=1\ 152s^4+96s^2+1$$

即

$$6a^2+b^2=1\ 152s^4+96s^2+1\tag{15}$$

由(14)式得

$$2a^2=\binom{2}{1}\times(24s^2+1)\times4s=8s(24s^2+1)$$

即

$$a^2=4s(24s^2+1)\tag{16}$$

由(16)式的 $a^2=4s(24s^2+1)$ 知 $2\mid a$.令 $a=2t$，$t\in\mathbb{Z}$，则(16)式变为

$$t^2=s(24s^2+1)\tag{17}$$

又因 $\gcd(s,24s^2+1)=1$，故(17)式可分解为：

$$s=c^2\qquad 24s^2+1=e^2\qquad t=ce\qquad \gcd(c,e)=1\tag{18}$$

将(18)式的 $s=c^2$ 代入 $24s^2+1=e^2$，得 $24c^4+1=e^2$，即

$$e^2-24c^4=1\tag{19}$$

因为方程(19)有正整数解$(e,c)=(5,1)$，故由文献[9]的定理1得方程(19)仅有正整数解$(e,c)=(5,1)$.于是 $s=c^2=1$，$1\ 152s^4+96s^2+1=1\ 249$，所以 $a^2=4s(24s^2+1)=100$，则 $a=10$.代入(16)式，得 $6a^2+b^2=600+b^2=1\ 249$，则有 $b^2=1\ 249-600=649$，显然无解，此时椭圆曲线(1)没有整数点.

当 $r=3$ 时，(4)式为 $12m^2-1=3a^4-8(6s^2-1)b^4$，将(3)式的 $m=ab$ 代入并配方，得

$$4(12s^2+1)b^4-3(a^2-2b^2)^2=1\tag{20}$$

令 $f=2b^2$，$t=a^2-2b^2$，$r,f\in\mathbb{N}$，则(20)式为

$$(12s^2+1)f^2-3t^2=1\tag{21}$$

又因$(1,2s)$为方程(21)的基本解，则方程(21)的一切整数解可表示为

$$f\sqrt{12s^2+1}+t\sqrt{3}=\pm(\sqrt{12s^2+1}+2s\sqrt{3})^{2n+1}\qquad n\in\mathbb{Z}$$

由此方程(20)的一切正整数解(b^2,a^2-2b^2)满足

$$2b^2\sqrt{12s^2+1}+|a^2-2b^2|\sqrt{3}=(\sqrt{12s^2+1}+2s\sqrt{3})^{2n+1}\qquad n\in\mathbb{N}\tag{22}$$

由(22)式，得

$$2b^2=\sum_{i=0}^{n}\binom{2n+1}{2i}\times\sqrt{12s^2+1}^{2(n-i)}\times(2s)^{2i}\times\sqrt{3}^{2i}=$$

$$(12s^2+1)+\sum_{i=1}^{n}\binom{2n+1}{2i}\times(12s^2+1)^{n-i}\times s^{2i}\times 3^i\times 4^i$$

即

$$2b^2=(12s^2+1)+\sum_{i=1}^{n}\binom{2n+1}{2i}\times(12s^2+1)^{n-i}\times s^{2i}\times 3^i\times 4^i \tag{23}$$

因为 $\sum_{i=1}^{n}\binom{2n+1}{2i}\times(12s^2+1)^{n-i}\times s^{2i}\times 3^i\times 4^i$ 为偶数，则(23)式左边为偶数，右边为奇数，矛盾，所以方程(23)无整数解，故 $r=3$ 时(3)式不成立，即情形 Ⅳ 不成立.

综上所述，定理 1 得证.

参考文献：

[1] 万　飞，杜先存. 关于不定方程 $x^3\pm 1=6pqDy^2$ 的整数解 [J]. 西南师范大学学报(自然科学版)，2016，41(12)：16－19.

[2] 呼家源，李小雪. Diophantine 方程 $x^3+8=py^2$ 有本原正整数解的必要条件 [J]. 西南大学学报(自然科学版)，2017，39(2)：50－54.

[3] ZAGIER D. Lager Integral Point on Elliptic Curves [J]. Math Comp，1987，48：425－436.

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

[5] 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.

[6] 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，2010：20－25.

[7] 管训贵. 椭圆曲线 $y^2=x^3+(p-4)x-2p$ 的整数点 [J]. 数学进展，2014，43(4)：521－526.

[8] 过　静. 椭圆曲线 $y^2=x^3+27x+62$ 的整数点 [J]. 重庆师范大学学报(自然科学版)，2016，33(5)：50－53.

[9] TOGBÉ A，VOUTIER P M，WALSH P G. Solving a Family of Thue 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 $y^2=(x+2)(x^2-2x+p)$

DU Xian-cun[1]，　ZHAO Jian-hong[2]，　WAN　Fei[1]

1. *College of Teacher Education，Honghe University，Mengzi Yunnan 661199，China*；
2. *Department of Mathematics and Computer Science，Lijiang Teachers College，Lijiang Yunnan 674199，China*

Abstract：Let $p=36s^2-5(s\in\mathbb{Z}_+,\ 2\nmid s)$，where is a positive odd number satisfying that $6s^2-1$ and $12s^2+1$ are primes. It is proved in this paper with the help of the Legendre symbol，congruence and some properties of the solutions to the Pell equation that the elliptic curve $y^2=(x+2)(x^2-2x+p)$ has only integer point $(x，y)=(-2，0)$.

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

责任编辑　廖　坤