DOI:10.13718/j.cnki.xsxb.2020.12.003

椭圆曲线 $y^2=x^3+(p-4)x-2p$ 的整数点①

李　萍[1]，　牟全武[1]，　瞿云云[2]

1. 西安工程大学 理学院，西安 710048；2. 贵州师范大学 数学科学学院，贵阳 550001

摘要：设 $p=81s^2+10$ 是素数，其中 s 是使 $9s^2+2$ 及 $\frac{9s^2+1}{2}$ 都是素数的正奇数. 运用初等数论的方法与技巧及四次丢番图方程的结果，证明了椭圆曲线 $y^2=x^3+(p-4)x-2p$ 仅有整数点 $(x,y)=(2,0)$.

关　键　词：椭圆曲线；整数点；二次剩余

中图分类号：O156.2　　**文献标志码**：A　　**文章编号**：1000-5471(2020)12-0010-05

文献[1]提出了求解椭圆曲线

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

整数点的问题. 文献[2]运用代数数论与 p-adic 分析方法证明了椭圆曲线(1)仅有整数点 $(x,y)=(2,0)$ 和(28 844 402，±154 914 585 540). 文献[3-4]对上述结果给出了一个简化证明.

对于一般的素数 p，找到椭圆曲线

$$y^2=x^3+(p-4)x-2p \tag{2}$$

的所有整数点是一个困难的数论问题. 设 s 是使 $12s^2+1$ 及 $6s^2-1$ 均为素数的正奇数，素数 p 可表示为 $p=36s^2-5$. 文献[5]在此假设下彻底解决了椭圆曲线(2)整数点的求解问题，这是对文献[2-4]所得结果的推广. 文献[6]证明了：当 p 满足一定条件时，椭圆曲线 $y^2=(x+2)(x^2-2x+p)$ 仅有整数点 $(x,y)=(-2,0)$. 文献[7]证明了：椭圆曲线 $y^2=x^3-17x+114$ 无正整数点. 文献[8]给出了三次丢番图方程 $x^3+8=py^2$ 有本原正整数解的必要条件.

本文证明了以下结果：

定理 1　设 $p=81s^2+10$ 是素数，其中 s 是使 $9s^2+2$ 及 $\frac{9s^2+1}{2}$ 都是素数的正奇数，则椭圆曲线(2)仅有整数点 $(x,y)=(2,0)$.

根据定理 1 可直接得到下述推论：

推论 1　椭圆曲线 $y^2=x^3+735x-1\,478$，$y^2=x^3+431\,655x-863\,318$ 均仅有整数点 $(x,y)=(2,0)$.

在本文里，用 $\mathbb{N}_+$ 表示全体正整数的集合，用 $\mathbb{Z}$ 表示全体整数的集合.

引理 1[9]　设 $D\geqslant 3$ 且不是完全平方数. 如果不定方程 $x^2-Dy^2=-2(x,y\in\mathbb{Z})$ 有解，且 $\lambda=x_0+y_0\sqrt{D}$ 为基本解，则该不定方程的全部正整数解可表示为

$$x+y\sqrt{D}=\frac{\lambda^{2n+1}}{2^n}\qquad n\in\mathbb{N}_+$$

① 收稿日期：2019-12-01

基金项目：陕西省自然科学基础研究计划项目(2019JM-337)；陕西省教育厅自然科学专项科研项目(17JK0341)；贵州省科学技术基金项目(黔科合基础[2019]1221 号)；贵州师范大学 2019 年博士科研启动项目(GZNUD[2019]13 号).

作者简介：李　萍(1974-)，女，副教授，主要从事初等数论与编码理论的研究.

引理 2[9-10]　设 D 是一个非平方的正整数. 又设(x_0, y_0) 是 Pell 方程

$$x^2-Dy^2=1 \tag{3}$$

的一组正整数解. 如果 $x_0>\frac{1}{2}y_0^2-1$，则 $x_0+y_0\sqrt{D}$ 是方程(3) 的基本解.

引理 3[9-10]　设 $x_0+y_0\sqrt{D}$ 是方程(3) 的基本解，则方程(3) 的全部正整数解可表示为

$$x+y\sqrt{D}=(x_0+y_0\sqrt{D})^n \qquad n\in\mathbb{N}_+$$

推论 2　设 s 为正奇数，则：

(i) 不定方程 $x^2-(9s^2+2)y^2=1$ 的基本解为 $9s^2+1+3s\sqrt{9s^2+2}$；

(ii) 不定方程 $x^2-36(9s^2+2)y^2=1$ 的基本解为$(9s^2+1+3s\sqrt{9s^2+2})^2$.

证　因为 $9s^2+2\equiv 2(\mathrm{mod}\ 3)$，且$\left(\frac{2}{3}\right)=-1$，所以 $9s^2+2$ 不是完全平方数. 由于$(x_0, y_0)=(9s^2+1, 3s)$ 是方程 $x^2-(9s^2+2)y^2=1$ 的正整数解，且满足 $x_0>\frac{1}{2}y_0^2-1$，根据引理 2 知结论(i) 成立. 由引理 3 及基本解的定义可得到结论(ii).

引理 4　若 D 是一个非平方的正整数，则不定方程

$$x^2-Dy^4=1 \tag{4}$$

至多有 2 组正整数解(x, y)，而且方程(4) 恰有两组正整数解的充要条件是 $D\in\{1\ 785, 28\ 560\}$，或者 $2x_0$ 和 y_0 都是平方数，这里(x_0, y_0) 是方程(3) 的基本解.

证　见文献[11] 的引理 2.

引理 5　若不定方程(4) 恰有一组正整数解，则这个唯一的正整数解(x, y) 可由下式表示：

$$x+y^2\sqrt{D}=(x_0+y_0\sqrt{D})^k$$

这里(x_0, y_0) 是方程(3) 的基本解，$k=2$，或 k 为正奇数.

证　见文献[12] 的定理 2.

定理 1 的证明

在以下叙述中，s 为正奇数，$p=81s^2+10$，$q=9s^2+2$，$r=\frac{9s^2+1}{2}$，其中 p,q,r 都是素数. 因为 $y^2=x^3+(p-4)x-2p=(x-2)(x^2+2x+p)$，所以椭圆曲线(2) 有平凡整数点$(x, y)=(2, 0)$. 下面仅考虑 $x>2$. 设 d 为 $x-2$ 与 x^2+2x+p 的最大公因数，则 $d=(x-2, x^2+2x+p)=(x-2, p+8)=(x-2, 9q)$. 注意 d 整除 $9q$，d 的取值只能是 $1,3,9,q,3q,9q$ 之一. 以下分情况讨论：

情形 1　若 $d=1$，即 $x-2$ 与 x^2+2x+p 互素，则存在正整数 a,b，使得

$$x-2=a^2 \qquad x^2+2x+p=b^2 \qquad y=\pm ab \qquad (a, b)=1$$

第二个等式即 $p-1=b^2-(x+1)^2$. 由于 b 与 $x+1$ 同奇偶，两边模 4 得 $2\equiv 0(\mathrm{mod}\ 4)$，矛盾.

情形 2　若 $d=3$，则存在正整数 a,b，使得

$$x-2=3a^2 \qquad x^2+2x+p=3b^2 \qquad y=\pm 3ab \qquad (a, b)=1$$

消去 x，整理得 $3[(a^2+1)^2+1+9s^2]=b^2$. 因为 3 不整除$(a^2+1)^2+1$，所以此等式左边不能是完全平方数，矛盾.

情形 3　若 $d=9$，则存在正整数 a,b，使得

$$x-2=9a^2 \qquad x^2+2x+p=9b^2 \qquad y=\pm 9ab \qquad (a, b)=1$$

消去 x，整理得 $9s^2+1=b^2-(3a^2+1)^2$，由此知 b 与 $3a^2+1$ 同奇偶. 对等式两边模 4 得 $2\equiv 0(\mathrm{mod}\ 4)$，矛盾.

情形 4　若 $d=q$，则存在正整数 a,b，使得

$$x-2=qa^2 \qquad x^2+2x+p=qb^2 \qquad y=\pm qab \qquad (a, b)=1$$

消去 x，整理得 $qa^4+6a^2+9=b^2$. 因为 a 与 b 互素，所以 3 不整除 a. 等式两边模 3，由费马小定理得 $b^2\equiv q\equiv 2(\mathrm{mod}\ 3)$，这与 $\left(\frac{2}{3}\right)=-1$ 矛盾.

情形 5　若 $d=3q$，则存在正整数 a,b，使得

$$x-2=3qa^2 \qquad x^2+2x+p=3qb^2 \qquad y=\pm 3qab \qquad (a,b)=1$$

消去 x，整理得 $3q(qa^4+2a^2+1)=b^2$，由此知 3 整除 b. 因为 a 与 b 互素，所以 a 与 3 互素. 因为 q 为大于 3 的素数，且 $qa^4+2a^2+1\equiv 2(\mathrm{mod}\ 3)$，即 $3q(qa^4+2a^2+1)$ 不能被 9 整除，所以 $3q(qa^4+2a^2+1)$ 不是完全平方数，这与等式右边矛盾.

情形 6　若 $d=9q$，则存在正整数 a,b，使得

$$x-2=9qa^2 \qquad x^2+2x+p=9qb^2 \qquad y=\pm 9qab \qquad (a,b)=1$$

消去 x，整理得

$$9(q-1)a^4+(3a^2+1)^2=b^2 \tag{5}$$

注意 $q-1$ 为偶数，由(5)式知 a 与 b 奇偶性不同. 若 a 为奇数，b 为偶数，则对等式(5)两边同时模 4 得 $q\equiv 1(\mathrm{mod}\ 4)$，这与 $q=9s^2+2\equiv 3(\mathrm{mod}\ 4)$ 矛盾. 所以 a 为偶数，b 为奇数. 不妨设 $a=2c$. 由(5)式得

$$288rc^4=b^2-(12c^2+1)^2=(b+12c^2+1)(b-12c^2-1) \tag{6}$$

设 $m=(b+12c^2+1,\ b-12c^2-1)$. 因为 b 与 $12c^2+1$ 奇偶性相同，所以 $2\mid m$. 若 $m>2$，则 $\frac{m}{2}$ 必有素因子 p_1. 由 $m\mid 2(12c^2+1)$ 得 $p_1\mid(12c^2+1)$. 又因为 $p_1\mid 288rc^4$ 且 $(288rc^4,\ 12c^2+1)=(r,\ 12c^2+1)$，所以 $p_1\mid r$. 因为 p_1 与 r 都是素数，必有 $p_1=r$，由此知 $12c^2\equiv -1(\mathrm{mod}\ r)$. 但这与 $\left(\frac{-12}{r}\right)=\left(\frac{-3}{r}\right)=-1$ 矛盾，故 $m=2$. 由(6)式可知，存在正整数 f,g,t，使得

$$b+(12c^2+1)=\frac{144r}{t}f^4 \qquad b-(12c^2+1)=2tg^4 \qquad c=fg \qquad \left(\frac{72r}{t}f^4,\ tg^4\right)=1 \tag{7}$$

其中 $t=1,8,9,72,r,8r,9r,72r$. 下面依次讨论这 8 种情形.

情形 6.1　$t=1$. 此时 $12c^2+1=72rf^4-g^4$. 等式两边取模 3，得 $g^4\equiv 2(\mathrm{mod}\ 3)$，这与 $\left(\frac{2}{3}\right)=-1$ 矛盾.

情形 6.2　$t=8$. 此时 $12c^2+1=9rf^4-8g^4$，g 与 3 互素. 由于 $c=fg$，$2r+1=q$，所以

$$(3f^2+4g^2)^2-q(3f^2)^2=-2$$

这意味着不定方程 $X^2-qY^2=-2$ 有解 $(X,Y)=(3f^2+4g^2,\ 3f^2)$. 注意不定方程 $X^2-qY^2=-2$ 的基本解为 $(X,Y)=(3s,\ 1)$，根据引理 1 知存在正整数 n，使得

$$3f^2+4g^2+3f^2\sqrt{q}=\frac{(3s+\sqrt{q})^{2n+1}}{2^n}$$

比较等式两边的有理部分，得

$$3f^2+4g^2=\frac{1}{2^n}\sum_{k=0}^{n}\binom{2n+1}{2k}(3s)^{2n+1-2k}q^k \tag{8}$$

(8)式左边不能被 3 整除，而右边是 3 的倍数，矛盾.

情形 6.3　$t=9$. 此时 $12c^2+1=8rf^4-9g^4$，将 $c=fg$ 及 $2r+1=q$ 代入并整理，得

$$(2f^2+3g^2)^2-4qf^4=-1$$

两边模 q 得

$$(2f^2+3g^2)^2\equiv -1(\mathrm{mod}\ q) \tag{9}$$

注意 $q=9s^2+2\equiv 3(\mathrm{mod}\ 4)$，同余式(9)不成立.

情形 6.4　$t=72$. 此时 $12c^2+1=rf^4-72g^4$，f 与 3 互素. 等式两边模 3，得 $r\equiv 1(\mathrm{mod}\ 3)$，这与 $r=$

$\frac{9s^2+1}{2}\equiv 2(\mathrm{mod}\ 3)$ 矛盾.

情形 6.5　$t=r$. 此时 $12c^2+1=72f^4-rg^4$，g 为奇数. 等式两边模 4，可推出 $r\equiv 3(\mathrm{mod}\ 4)$，这与 $r=\frac{9s^2+1}{2}\equiv 1(\mathrm{mod}\ 4)$ 矛盾.

情形 6.6　$t=8r$. 此时 $12c^2+1=9f^4-8rg^4$，g 与 3 互素. 将 $c=fg$ 及 $r=\frac{q-1}{2}$ 代入并整理，得 $(3f^2-2g^2)^2-4qg^4=1$. 这说明 Pell 方程

$$X^2-qY^2=1 \tag{10}$$

有特解 $(X,Y)=(|3f^2-2g^2|,2g^2)$. 从推论 2 的(i)知 $9s^2+1+3s\sqrt{q}$ 为方程(10)的基本解，所以由引理 3 知存在正整数 n，使得

$$|3f^2-2g^2|+2g^2\sqrt{q}=(9s^2+1+3s\sqrt{q})^n$$

比较等式两边 $\sqrt{q}$ 的系数，得

$$2g^2=\sum_{k=1}^{\left[\frac{n+1}{2}\right]}\binom{n}{2k-1}(9s^2+1)^{n-2k+1}(3s)^{2k-1}q^{k-1}$$

上式右端显然能被 3 整除，由此得 $3\mid g$，这与 g 和 3 互素矛盾.

情形 6.7　$t=9r$. 此时 $12c^2+1=8f^4-9rg^4$，f 与 3 互素. 等式两边模 3 并利用费马小定理，得 $1\equiv 2(\mathrm{mod}\ 3)$，这不成立.

情形 6.8　$t=72r$. 此时有

$$12c^2+1=f^4-72rg^4 \tag{11}$$

其中 f 为奇数且与 3 互素. 与情形 6.6 类似，(11)式可化简为 $(f^2-6g^2)^2-36qg^4=1$. 这意味着 Pell 方程

$$x^2-36qy^4=1 \tag{12}$$

有正整数解 $(x,y)=(|f^2-6g^2|,g)$. 由推论 2 的结论(ii)及引理 4 知方程(12)仅有 1 组正整数解 $(x,y)=(|f^2-6g^2|,g)$，因此根据引理 5 知

$$|f^2-6g^2|+6g^2\sqrt{q}=(9s^2+1+3s\sqrt{q})^{2k} \tag{13}$$

其中 $k=2$，或 k 为正奇数. 注意 $9s^2+1=2r$，比较等式(13)两边 $\sqrt{q}$ 的系数，得

$$6g^2=\sum_{j=1}^{k}\binom{2k}{2j-1}(2r)^{2k-2j+1}(3s)^{2j-1}q^{j-1}$$

即

$$g^2=rs\sum_{j=1}^{k}\binom{2k}{2j-1}(2r)^{2(k-j)}(9qs^2)^{j-1} \tag{14}$$

若 $k=2$，由(14)式可得 $g^2=4rs(4r^2+9qs^2)$. 注意 r 为素数且 r 与 $s(4r^2+9qs^2)$ 互素，故 $4rs(4r^2+9qs^2)$ 不是完全平方数，矛盾. 若 k 为正奇数，将(14)式写为

$$g^2=rs\left[2k(9qs^2)^{k-1}+\sum_{j=1}^{k-1}\binom{2k}{2j-1}(2r)^{2(k-j)}(9qs^2)^{j-1}\right] \tag{15}$$

(15)式右端为偶数，但由 r,s,k,q 都是奇数知右端不能被 4 整数，故不是完全平方数，这与左端矛盾.

综上所述，定理 1 得证.

参考文献：

[1] ZAGIER D. Large Integral Points on Elliptic Curves [J]. Math Comp, 1987, 48(177): 425-436.

[2] ZHU H L, CHEN J H. Integral Points on $y^2=x^3+27x-62$ [J]. 数学研究, 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.

[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，2010：20-25.
[5] 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.
[6] 杜先存，赵建红，万 飞. 椭圆曲线 $y^2=(x+2)(x^2-2x+p)$ 的整数点[J]. 西南大学学报(自然科学版)，2017，39(6)：69-73.
[7] 赵建红，杜先存. 椭圆曲线 $y^2=x^3-17x+114$ 的正整数点[J]. 西南师范大学学报(自然科学版)，2018，43(4)：11-14.
[8] 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.
[9] 曹珍富. 不定方程及其应用[M]. 上海：上海交通大学出版社，2000：1-28.
[10] 柯 召，孙 琦. 谈谈不定方程[M]. 哈尔滨：哈尔滨工业大学出版社，2011：15-30.
[11] WALSH G. A Note on a Theorem of Ljunggren and the Diophantine Equations $x^2-kxy^2+y^4=1,4$ [J]. Arch Math，1999，73(2)：119-125.
[12] 罗家贵，袁平之. 关于不定方程 $x^2-Dy^4=1$ [J]. 四川大学学报(自然科学版)，2001，38(1)：1-5.

Integral Points on Elliptic Curve $y^2=x^3+(p-4)x-2p$

LI Ping[1]， MU Quan-wu[1]， QU Yun-yun[2]

1. *School of Science，Xi'an Polytechnic University，Xi'an 710048，China*；
2. *School of Mathematical Science，Guizhou Normal University，Guiyang 550001，China*

Abstract：Let $p=81s^2+10$ be a prime，where s is a positive odd number satisfying that $9s^2+2$ and $\frac{9s^2+1}{2}$ are primes. By combining some methods and techniques of elementary number theory with some known results of quartic diophantine equations，it is proved that the elliptic curve $y^2=x^3+(p-4)x-2p$ has only the integral point $(x,y)=(2,0)$.

Key words：elliptic curve；integral point；quadratic residues

责任编辑 廖 坤