文章编号：1000－5471(2011)01－0034－05

孪生素数椭圆曲线在 $p=5$ 时的整数点①

陈 候 炎

湛江师范学院 基础教育学院，广东 湛江 524300

摘要：运用初等数论方法证明了：孪生素数椭圆曲线 E_-：$y^2=x(x-5)(x-7)$ 仅有整数点(0，0)，(5，0)和(7，0)；E_+：$y^2=x(x+5)(x+7)$ 仅有整数点(0，0)，(－5，0)，(－7，0).

关　键　词：孪生素数椭圆曲线；整数点；Diophantine 方程

中图分类号：O156　　**文献标志码**：A

确定椭圆曲线整数点是数论和算术代数几何学的有趣问题. 为了解决这些问题，近几年出现了很多先进方法[1－3]，本文提出另一种解决方法.

下文中约定，$\mathbf{Z}$，$\mathbf{N}^+$ 分别是全体整数的集合和全体正整数的集合，p 和 q 是一对孪生素数且 $p+2=q$. 文献[4－5]确定了 Mordell-Weil 群和椭圆曲线

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

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

的秩，并给出式(1)和式(2)的某些情形的整数点的结论(为方便计，以下记式(1)为 E_-，式(2)为 E_+). 事实上，他们证明了：如果 $p\equiv\pm 3\pmod 8$，那么 E_- 没有形如

$$(x,y)=(pqa^2,\pm pqabc)\qquad a,b,c\in\mathbf{N}^+$$

的整数点. 后来，文献[6]进一步研究上述结论，去掉了“$p\equiv\pm 3\pmod 8$”的约束条件.

显然，确定孪生素数椭圆曲线的所有整数点非常困难，本文运用简洁的初等数论的方法完全解决了 $p=5$ 的情形. 即证明了以下两个定理.

定理 1　当 $p=5$ 时，E_- 仅有整数点(0，0)，(5，0)，(7，0).

定理 2　当 $p=5$ 时，E_+ 仅有整数点(0，0)，(－5，0)，(－7，0).

1　几个引理

引理 1　方程

$$X^2-DY^4=1\qquad X,Y\in\mathbf{N}^+ \tag{3}$$

最多有两个解. 进一步，当 $D\neq 1785$ 或 $D\neq 28560$，而(3)恰有两个解时，有 $u_1=2r^2$，$v_1=s^2$，其中 r 和 s 是正整数.

证　见文献[7]的定理 1.

引理 2　方程

① 收稿日期：2010－01－10
基金项目：国家自然科学基金资助项目(10971184；10771186).
作者简介：陈候炎(1969－)，男，广东湛江人，高级讲师，硕士，主要从事代数数论的研究.

$$4X^2-35Y^4=1 \qquad X,Y\in \mathbf{N}^+ \tag{4}$$

恰有一个整数解$(X,Y)=(3,1)$.

证　显然，$2\nmid Y$.

当 $Y=1$ 时，方程(4) 有整数解$(X,Y)=(3,1)$.

当 $Y\geqslant 3$ 时，若方程(4) 有整数解(X,Y)，则 $4X^2-1=35Y^4$. 令 $A=2X+1$，$B=2X-1$，则 $\gcd(A,B)=1$，$A\cdot B=35Y^4$，$A-B=2$. 故 A,B 不可能同时含有因子 Y. 而 $Y^4>80$，所以(4) 无整数解.

引理 3　当素数 $p\not\equiv 1,3,9,15 \pmod{16}$ 时，丢番图方程 $X^2-8pY^4=1$ 没有正整数解.

证　见文献[8] 的定理 4.

2　定理 1 的证明

当 $p=5$ 时，E_- 可写成

$$y^2=x(x-5)(x-7) \tag{5}$$

显然，当 $y=0$ 时，式(5) 只有整数点$(0,0)$，$(5,0)$，$(7,0)$.

以下，我们只要证明当 $y\neq 0$ 时，式(5) 没有整数点即可.

当 $y\neq 0$ 时，假设(x,y) 是式(5) 的一个整数点.

因为 $y^2>0$，所以，由式(5) 得 $0<x<5$ 或 $x>7$.

如果 $0<x<5$，那么，当 $x=1$ 时，$y^2=24$；当 $x=2$ 时，$y^2=30$；当 $x=3$ 时，$y^2=24$；当 $x=4$ 时，$y^2=12$. 这都与 y 是整数矛盾.

因此，我们有 $x>7$.

设 $d_1=\gcd(x,x-5)$，$d_2=\gcd(x,x-7)$，$d_3=\gcd(x-5,x-7)$，于是

$$d_1=\begin{cases}1 & 5\nmid x\\ 5 & 5\mid x\end{cases}\qquad d_2=\begin{cases}1 & 7\nmid x\\ 7 & 7\mid x\end{cases}\qquad d_3=\begin{cases}1 & 2\nmid x\\ 2 & 2\mid x\end{cases} \tag{6}$$

设 a,b,c 是两两互素的正整数. 由式(6)，我们只需讨论以下 8 种情形.

情形 1　$(d_1,d_2,d_3)=(1,1,1)$

由式(5)，取

$$x=a^2 \qquad x-5=b^2 \qquad x-7=c^2 \qquad y=\pm abc \tag{7}$$

由此得，$2=(x-5)-(x-7)=b^2-c^2\geqslant b+c>2$，矛盾.

运用证明情形 1 的方法，可证明以下 3 种情形.

情形 2　$(d_1,d_2,d_3)=(5,1,1)$

情形 3　$(d_1,d_2,d_3)=(1,7,1)$

情形 4　$(d_1,d_2,d_3)=(1,1,2)$

下面证明其余几种情形.

情形 5　$(d_1,d_2,d_3)=(5,7,1)$

取

$$x=35a^2 \qquad x-5=5b^2 \qquad x-7=7c^2 \qquad y=\pm 35abc \tag{8}$$

由此可得，$7a^2-b^2=1$. 但，因为 $7\nmid b$，故 $b^2+1\equiv 2,3,5 \pmod 7$，这不可能.

情形 6　$(d_1,d_2,d_3)=(1,7,2)$

可令

$$x=7a^2 \qquad x-5=2b^2 \qquad x-7=14c^2 \qquad y=\pm 14abc \tag{9}$$

由此可知

$$a^2-2c^2=1 \qquad b^2-7c^2=1 \tag{10}$$

进而，由式(9) 和式(10) 知 $2\nmid a$，$2\nmid b$，$2\mid c$，且

$$b^2-a^2=5c^2 \tag{11}$$

从而，由式(11)，可得

$$b+a=\begin{cases}10f^2\\2g^2\end{cases}\qquad b-a=\begin{cases}2g^2\\10f^2\end{cases}\qquad c=2fg\qquad f,g\in\mathbf{N}^+ \tag{12}$$

由此可得

$$c=2fg\qquad b=5f^2+g^2\qquad a=|5f^2-g^2| \tag{13}$$

将式(13)代入式(10)的第一个等式，可得

$$(9f^2-g^2)^2-56g^4=1 \tag{14}$$

然而，由引理3知，方程(14)无整数解.

情形7 $(d_1,d_2,d_3)=(5,1,2)$

令

$$x=5a^2\qquad x-5=10b^2\qquad x-7=2c^2\qquad y=\pm 10abc \tag{15}$$

由此可知

$$a^2-2b^2=1\qquad 5a^2-7=2c^2 \tag{16}$$

且

$$c^2-5b^2=-1 \tag{17}$$

故由式(16)得$2\nmid a$. 可设$a=2k-1$，则

$$2b^2=(2k-1)^2-1=4k(k-1) \tag{18}$$

则$2\mid b$，故$2\nmid c$. 可设$b=2l$，$c=2t-1$，代入式(14)，有

$$8l^2=(2t-1)^2+1=4t(t-1)+2 \tag{19}$$

这是不可能的.

情形8 $(d_1,d_2,d_3)=(5,7,2)$

设

$$x=35a^2\qquad x-5=10b^2\qquad x-7=14c^2\qquad y=\pm 70abc \tag{20}$$

由此可得

$$7c^2-5b^2=-1 \tag{21}$$

但，因为$5\nmid c$，故$7c^2+1\equiv 3,4\pmod 5$，而$5b^2\equiv 0\pmod 5$，矛盾. 所以，式(21)不可能成立.

综上所述，当$y\neq 0$时，式(5)没有整数点(x,y).

3 定理2的证明

设$p=5$，则E_+可表示为

$$y^2=x(x+5)(x+7) \tag{22}$$

显然，当$y=0$时，式(22)仅有整数点$(0,0)$，$(-5,0)$，$(-7,0)$.

设(x,y)(其中$y\neq 0$)是式(22)的一个整数点. 因为$y^2>0$，故由式(22)得$-7<x<-5$或$x>0$.

如果$-7<x<-5$，那么$x=-6$，$y^2=6$. 故当$x<0$时，式(22)无整数点.

下设$x>0$.

令$d_1=\gcd(x,x+5)$，$d_2=\gcd(x,x+7)$，$d_3=\gcd(x+5,x+7)$. 则d_1,d_2,d_3满足式(6). 所以，仿定理1的证明，只讨论以下8种情形.

情形1 $(d_1,d_2,d_3)=(1,1,1)$

取

$$x=a^2\qquad x+5=b^2\qquad x+7=c^2\qquad y=\pm abc \tag{23}$$

可得$2=(x+7)-(x+5)=c^2-b^2\geqslant c+b>2$，矛盾.

用同样的方法可证明以下 3 种情形也是不可能的.

情形 2　$(d_1, d_2, d_3)=(5, 1, 1)$

情形 3　$(d_1, d_2, d_3)=(1, 7, 1)$

情形 4　$(d_1, d_2, d_3)=(1, 1, 2)$

下面证明其余几种情形.

情形 5　$(d_1, d_2, d_3)=(5, 7, 1)$

记

$$x=35a^2 \qquad x+5=5b^2 \qquad x+7=7c^2 \qquad y=\pm 35abc \tag{24}$$

由此可得

$$c^2-5a^2=1 \qquad b^2-7a^2=1 \tag{25}$$

进而，由式(24) 和式(25) 知 $2\mid a$，$2\nmid b$，$2\nmid c$，且

$$b^2-c^2=2a^2 \tag{26}$$

从而，由式(26) 可得

$$b+c=\begin{cases}4f^2\\2g^2\end{cases} \qquad b-c=\begin{cases}2g^2\\4f^2\end{cases} \qquad a=2fg \qquad f,g\in \mathbf{N}^+ \tag{27}$$

由此可得

$$a=2fg \qquad b=2f^2+g^2 \qquad c=\mid 2f^2-g^2\mid \tag{28}$$

将式(28) 代入式(27) 的第一个等式，可得

$$4(f^2-3g^2)^2-35g^4=1 \tag{29}$$

然而，由引理 2 知，方程 $4X^2-35Y^4=1$ 只有唯一解 $(X, Y)=(3, 1)$，因此，式(29) 无整数解.

情形 6　$(d_1, d_2, d_3)=(1, 7, 2)$

可设

$$x=7a^2 \qquad x+5=2b^2 \qquad x+7=14c^2 \qquad y=\pm 14abc \tag{30}$$

由此可知

$$a^2-2c^2=-1 \qquad b^2-7c^2=-1 \tag{31}$$

进而，由式(30) 和式(31) 可得 $7\nmid b$，即 $b^2+1\equiv 2,3,5 \pmod 7$，矛盾.

情形 7　$(d_1, d_2, d_3)=(5, 1, 2)$

设

$$x=5a^2 \qquad x+5=10b^2 \qquad x+7=2c^2 \qquad y=\pm 10abc \tag{32}$$

由此可知

$$a^2-2b^2=-1 \tag{33}$$

且

$$5a^2+7=2c^2 \tag{34}$$

故由式(33) 和式(34) 得 $2\nmid a$. 可设 $a=2k-1$，代入式(34)，得

$$2c^2=5(2k-1)^2+7=20k(k-1)+12 \tag{35}$$

则 $2\mid c$. 可设 $c=2l$，代入式(35)，得

$$2l^2=5k(k-1)+3 \tag{36}$$

这是不可能的.

情形 8　$(d_1, d_2, d_3)=(5, 7, 2)$

记

$$x=35a^2 \qquad x+5=10b^2 \qquad x+7=14c^2 \qquad y=\pm 70abc \tag{37}$$

可得

$$7c^2-5b^2=1 \tag{38}$$

由于 $5\nmid c$，故 $7c^2-1\equiv 1,2 \pmod 5$，而 $5b^2\equiv 0 \pmod 5$，矛盾.

综上所述，定理2得证.

参考文献：

[1] BAKER A. The Diophantine Equation $y^2=ax^3+bx^2+cx+d$ [J]. J London Math Soc, 1968, 43(1): 1－9.

[2] STROEKER R J, TZANAKIS N. Solving Elliptic Diophantine Equations by Estimating Linear Forms in Elliptic Logarithms [J]. Acta Arith, 1994, 67(2): 177－196.

[3] STROEKER R J, TZANAKIS N. Computing All Integer Solutions of a Genus 1 Equation [J]. Math Comp, 2003, 72(9): 1917－1933.

[4] QIU De-rong, ZHANG Xian-ke. Elliptic Curves of Twin-Primes Over Gauss Field and Diophantine Equations [J]. 数学进展, 2000, 29(3): 279－281.

[5] QIU De-rong, ZHANG Xian-ke. Mordell-Weil Groups and Selmer Groups of Twin-Prime Elliptic Curves [J]. Sci China: Ser A, 2002, 45(11): 1372－1380.

[6] LE Mao-hua. On the Simultaneous Pell Equation $x^2-D_1y^2=\delta$ and $z^2-D_2y^2=\delta$ [J]. 数学进展, 2001, 30(1): 87－88.

[7] 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.

[8] 潘家宇. 关于丢番图方程 $x^2-Dy^4=1$ 的一些注记 [J]. 河南科学, 1997, 15(1): 18－22.

[9] 罗 明，朱德辉，马芙蓉. 关于不定方程 $3x(x+1)(x+2)(x+3)=5y(y+1)(y+2)(y+3)$ [J]. 西南师范大学学报：自然科学版, 2009, 34(5): 16－21.

[10] 罗 明，黄勇庆. 关于不定方程 $x^3-1=26y^2$ [J]. 西南大学学报：自然科学版, 2007, 29(6): 5－7.

Integral Points on Twin Primes Elliptic Curves for $p=5$

CHEN Hou-yan

College of Basic Education, Zhanjiang Normal University, ZhanJiang Guangdong, 524300, China

Abstract: Using elementary number theory methods, it was proved that the twin prime elliptic curve $y^2=x(x-5)(x-7)$ and $y^2=x(x+5)(x+7)$ have only the integral points (0, 0), (5, 0), (7, 0) and (0, 0), (－5, 0), (－7, 0) respectively.

Key words: twin prime elliptic curve; integral point; Diophantine equation

责任编辑 覃吉康