文章编号　1000-5269(2022)06-0025-06　　DOI:10.15958/j.cnki.gdxbzrb.2022.06.03

关于不定方程 $x^2-pqy^4=16$ 的正整数解

管训贵,潘小明*
(泰州学院 数理学院,江苏 泰州 225300)

摘　要:设 p,q 为奇素数,m 为大于 1 的整数,满足 $q=p+2^m$。为了研究椭圆曲线 $y^2=x(x+\varepsilon p)(x+\varepsilon q)$($\varepsilon\in\{-1,1\}$)的整数点,曾有不少学者对不定方程 $x^2-pqy^4=2^n$($n\in\mathbf{N}^*$)的正整数解产生兴趣。利用同余式、平方剩余、Pell 方程解的性质、递归序列,研究了不定方程 G:$x^2-pqy^4=16$ 的正整数解问题,并给出 $(p,q)=(5,11),(11,19)$ 以及 $(5,13)$ 时,G 的全部正整数解。

关键词:不定方程;奇素数;正整数解;同余式;平方剩余;递归序列
中图分类号:O156.1　　**文献标志码**:A

设 p,q 为奇素数,m 为大于 1 的整数,满足 $q=p+2^m$。有一类典型的椭圆曲线是

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

在确定式(1)的整数点时,曾分解出一种情形:

$$x=pqa^2,x+\varepsilon p=2^spb^2$$

$$x+\varepsilon q=2^sqc^2,y=\pm 2^spqabc$$

此情形最终归结为讨论不定方程

$$(2^{s+1}u^2-(2^{m-1}+\varepsilon p)v_1^2)^2-pqv_1^4=2^{s+2},0\leqslant s\leqslant 2$$

的正整数解。当 $s=0,1$ 时,此方程的讨论比较简单;而 $s=2$ 时,则较为复杂。基于上述考虑,本文讨论不定方程

$$x^2-pqy^4=16,\gcd(x,y)=1,x,y\in\mathbf{N}^*\tag{2}$$

的解。当然,式(2)也是不定方程的基本类型之一[1-3]。本文用初等方法对式(2)的解进行了探究,获得以下一般性的结果。

1　主要结论

定理　设 p,q 为奇素数,m 为大于 1 的整数,且 $q=p+2^m$。若不定方程

$$X^2-pqY^2=16,\gcd(X,Y)=1,X,Y\in\mathbf{N}^*$$

的解仅有 2 个非结合类,而 $u_n+v_n\sqrt{pq}$ 为 Pell 方程 $U^2-pqV^2=1$ 的非负整数解,适合

$$u_1\equiv 3(\bmod 4),v_1\equiv 2(\bmod 4)$$

或

$$u_1\not\equiv 3(\bmod 8),v_1\equiv 4(\bmod 8)$$

或

$$u_1\not\equiv 7(\bmod 8),v_1\equiv 0(\bmod 8)$$

则式(2)的解必满足

$$y^2=u_n+(p+2^{m-1})v_n,n\geqslant 0$$

根据定理直接可得:

推论 1　不定方程

$$x^2-33y^4=16,x,y\in\mathbf{N}^*\tag{3}$$

仅有解 $(x,y)=(7,1)$ 和$(92,4)$。

推论 2　不定方程

$$x^2-209y^4=16,x,y\in\mathbf{N}^*\tag{4}$$

仅有解 $(x,y)=(15,1)$。

推论 3　不定方程

$$x^2-65y^4=16,x,y\in\mathbf{N}^*\tag{5}$$

仅有解 $(x,y)=(9,1)$ 和$(516,8)$。

2　一些引理

引理 1[4]　设 $D>0$ 且不是平方数,$X_1+Y_1\sqrt{D}$ 是不定方程

$$X^2-DY^2=M,M\in\mathbf{N}^*\tag{6}$$

的某结合类 k 的最小正整数解,$u_1+v_1\sqrt{D}$ 是 Pell 方程 $U^2-DV^2=1$ 的基本解,则

$$0<Y_1\leqslant\frac{v_1\sqrt{M}}{\sqrt{2(u_1+1)}}$$

收稿日期:2022-01-19
基金项目:江苏省自然科学基金资助项目(BK20171318);江苏省教育科学“十三五”规划课题(D20200115);江苏省“青蓝工程”数学教育教学团队资助项目(SJS201903)
作者简介:管训贵(1963—),男,教授,研究方向:数论,E-mail:tzszgxg@126.com.
*通讯作者:潘小明,E-mail:panxiaoming2080@sina.com.

引理 2[4] 不定方程(6)的整数解仅有有限个结合类。设 $X_1 + Y_1\sqrt{D}$ 是类 k 的最小正整数解,则类 k 的一切整数解可表示为

$$X + Y\sqrt{D} = \pm (X_1 + Y_1\sqrt{D})(u_1 + v_1\sqrt{D})^n$$

这里, $u_1 + v_1\sqrt{D}$ 是 Pell 方程 $U^2 - DV^2 = 1$ 的基本解, $n \in \mathbf{Z}$。

引理 3[4] 设 $D > 0$ 且不是平方数, $a + b\sqrt{D}$ 是 Pell 方程 $U^2 - DV^2 = 1$ 的基本解, $u_n + v_n\sqrt{D}$ 为其任一整数解,则有

(ⅰ) $u_{n+2} = 2au_{n+1} - u_n, u_0 = 1, u_1 = a$; $v_{n+2} = 2av_{n+1} - v_n, v_0 = 0, v_1 = b$。

(ⅱ) $u_{2n} = u_n^2 + Dv_n^2 = 2u_n^2 - 1 = 2Dv_n^2 + 1$, $v_{2n} = 2u_nv_n$。

(ⅲ) $u_{-n} = u_n, v_{-n} = -v_n$。

(ⅳ) $u_{3n} = u_n(4u_n^2 - 3), v_{3n} = v_n(4u_n^2 - 1)$。

(ⅴ) $u_{n+2km} \equiv (-1)^k u_n \pmod{u_m}$; $v_{n+2km} \equiv (-1)^k v_n \pmod{u_m}$。

引理 4[5] 设 $D > 0$ 且不是平方数,则不定方程

$$x^2 - Dy^4 = 1 \tag{7}$$

至多有两组正整数解 (x,y)。若式(7)恰有两组正整数解,则当 $D \neq 1\,785,28\,560$ 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。若式(7)仅有一组正整数解 (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。

由引理 4 即得引理 5。

引理 5 不定方程 $x^2 - 33y^4 = 1$ 仅有正整数解 $(x,y) = (23,2)$。

证明 因为 $33 \neq 1\,785,28\,560$, 且 $v_2 = 2^3 \times 23$ 为非平方数,故由引理 4 知,该不定方程至多有一组正整数解。又由 $23^2 - 33 \times 2^4 = 1$ 知结论成立。证毕。

类似可证引理 6。

引理 6 不定方程 $x^2 - 65y^4 = 1$ 仅有正整数解 $(x,y) = (129,4)$。

引理 7[6] 设 p,q 为不同的奇素数,若 $p \equiv 3 \pmod 4$, $q \equiv 3 \pmod 4$, 则不定方程 $x^4 - pqy^2 = 1$ 没有正整数解 (x,y)。

引理 8[7] 设整数 $a > 1$, 则不定方程

$$ax^2 - Dy^4 = 1 \tag{8}$$

至多有 1 组正整数解。若 (x,y) 是式(8)的正整数解,则不定方程 $aU^2 - DV^2 = 1$ 有正整数解,它的基本解 (u_1,v_1) 中 v_1 的无平方因子部分 l 是奇数,而且 $(x,y) = (u_l,\sqrt{v_l})$。

引理 9 不定方程

$$x^2 - 836y^4 = 1 \tag{9}$$

无正整数解 (x,y)。

证明 设 (x,y) 是式(9)的任一正整数解。由 $2 \nmid x$ 知, $\gcd(x+1, x-1) = 2$, 故有

$$x + 1 = 418r^4, x - 1 = 2s^4 \tag{10}$$

或

$$x + 1 = 2s^4, x - 1 = 418r^4 \tag{11}$$

或

$$x + 1 = 38r^4, x - 1 = 22s^4 \tag{12}$$

或

$$x + 1 = 22s^4, x - 1 = 38r^4 \tag{13}$$

这里, $s,r \in \mathbf{N}^*, \gcd(s,r) = 1, y = rs$。

若式(10)成立,则得 $s^4 - 209r^4 = -1$。取模 11,有 $s^4 \equiv -1 \pmod{11}$, 不可能。

若式(11)成立,则得 $s^4 - 209r^4 = 1$。由于 $11 \equiv 3 \pmod 4, 19 \equiv 3 \pmod 4$, 故由引理 7 知,不可能。

若式(12)成立,则得 $11s^4 - 19r^4 = -1$。取模 11 得 $19r^4 \equiv 1 \pmod{11}$。但 $(\frac{19}{11}) = -1$, 不可能。

若式(13)成立,则得

$$11s^4 - 19r^4 = 1 \tag{14}$$

易知 $11U^2 - 19V^2 = 1$ 的最小正整数解为 $(u_1,v_1) = (46,35)$。根据引理 8,要使式(14)有正整数解,必须 $(s^2,t) = (u_{35}, \sqrt{v_{35}})$。因为

$$\begin{aligned} u_n\sqrt{11} + v_n\sqrt{19} &= (46\sqrt{11} + 35\sqrt{19})(46\,551 + 3\,220\sqrt{209})^n \\ &= (46\sqrt{11} + 35\sqrt{19})(x_n + y_n\sqrt{209}) \end{aligned}$$

这里, $n \geqslant 0, 46\,551 + 3\,220\sqrt{209}$ 是 Pell 方程 $x^2 - 209y^2 = 1$ 的基本解,所以

$$v_n = 35x_n + 506y_n \tag{15}$$

并且有序列:

$$\begin{aligned} x_{n+2} &= 93\,102x_{n+1} - x_n, x_0 = 1, x_1 = 46\,551 \\ y_{n+2} &= 93\,102y_{n+1} - y_n, y_0 = 0, y_1 = 3\,220 \end{aligned} \tag{16}$$

利用式(16)对式(15)取模 8,得 $v_{35} \equiv 5 \pmod 8$, 即 v_{35} 不是完全平方数。因此,式(14)无正整数解。证毕。

引理 10　不定方程

$$x^2-209y^4=1 \tag{17}$$

无正整数解 (x,y)。

证明　设 (x,y) 是式(17)的任一正整数解。若 $2\nmid y$, 则对式(17)取模 8,得 $x^2\equiv 2(\bmod 8)$, 不可能, 故 $2\mid y$, 从而 $2\nmid x$。此时 $\gcd(x-1,x+1)=2$, 故有

$$x+1=1\,672r^4,x-1=2s^4 \tag{18}$$

或

$$x+1=2s^4,x-1=1\,672r^4 \tag{19}$$

或

$$x+1=418r^4,x-1=8s^4 \tag{20}$$

或

$$x+1=8s^4,x-1=418r^4 \tag{21}$$

或

$$x+1=152r^4,x-1=22s^4 \tag{22}$$

或

$$x+1=22s^4,x-1=152r^4 \tag{23}$$

或

$$x+1=88r^4,x-1=38s^4 \tag{24}$$

或

$$x+1=38s^4,x-1=88r^4 \tag{25}$$

这里, $s,r\in\mathbf{N}^*,\gcd(s,r)=1,y=2rs$。

若式(18)成立,则得 $s^4-836r^4=-1$。取模 11,有 $s^4\equiv -1(\bmod 11)$, 不可能。

若式(19)成立,则得 $s^4-836r^4=1$。根据引理 9 知,不可能。

若式(20)成立,则得 $4s^4-209r^4=-1$。取模 11,有 $4s^4\equiv -1(\bmod 11)$, 不可能。

若式(21)成立,则得 $4s^4-209r^4=1$。取模 4,有 $r^4\equiv -1(\bmod 4)$, 不可能。

若式(22)成立,则得 $11s^4-76r^4=-1$。取模 19,有 $(11s^2)^2\equiv -11(\bmod 19)$, 但 $\left(\frac{-11}{19}\right)=\left(\frac{8}{19}\right)=\left(\frac{2}{19}\right)=-1$, 不可能。

若式(23)成立,则得 $11s^4-76r^4=1$。取模 4,有 $s^4\equiv -1(\bmod 4)$, 不可能。

若式(24)成立,则得 $19s^4-44r^4=-1$。取模 19,有 $(22r^2)^2\equiv -11(\bmod 19)$, 但 $\left(\frac{-11}{19}\right)=-1$, 不可能。

若式(25)成立,则得 $19s^4-44r^4=1$。取模 4,有 $s^4\equiv -1(\bmod 4)$, 不可能。

因此,式(17)无正整数解。证毕。

3　定理的证明

因为 $(p+2^{m-1})^2-p(p+2^m)\cdot 1^2=16$, 且不定方程

$$X^2-pqY^2=16,\ \gcd(X,Y)=1,\ X,Y\in\mathbf{N}^* \tag{26}$$

仅有 2 个非结合类的解,所以根据引理 2,式(26)的一般解可表示为

$$\begin{aligned}X+Y\sqrt{pq}&=\pm(p+2^{m-1}+\sqrt{pq})(u_n+v_n\sqrt{pq})\\&=\pm(p+2^{m-1}+\sqrt{pq})(a+b\sqrt{pq})^n\end{aligned}$$

或

$$\begin{aligned}X+Y\sqrt{pq}&=\pm(-p-2^{m-1}+\sqrt{pq})(u_n+v_n\sqrt{pq})\\&=\pm(-p-2^{m-1}+\sqrt{pq})(a+b\sqrt{pq})^n\end{aligned}$$

这里, $n\in\mathbf{Z},p+2^{m-1}+\sqrt{pq}$ 为方程 $X^2-pqY^2=16$ 的最小正整数解, $a+b\sqrt{pq}$ 为 Pell 方程 $U^2-pqV^2=1$ 的基本解。

若式(2)有解,必有 n, 使得

$$y^2=\pm(u_n+(p+2^{m-1})v_n)$$

或

$$\begin{aligned}y^2&=\pm(u_n-(p+2^{m-1})v_n)\\&=\pm(u_{-n}+(p+2^{m-1})v_{-n})\end{aligned}$$

当 $n\geqslant 0$ 时, $u_n+(p+2^{m-1})v_n>0$;当 $n<0$ 时, $u_n+(p+2^{m-1})v_n<0$。因此可归结为:

$$y^2=u_n+(p+2^{m-1})v_n,n\geqslant 0 \tag{27}$$

或

$$y^2=-u_n+(p+2^{m-1})v_n,n>0 \tag{28}$$

由引理 3 的(ⅰ)知:

$$u_{n+2}=2au_{n+1}-u_n,u_0=1,u_1=a \tag{29}$$

$$v_{n+2}=2av_{n+1}-v_n,v_0=0,v_1=b \tag{30}$$

当 $u_1\equiv 3(\bmod 4),v_1\equiv 2(\bmod 4)$ 时, 对式(29)取模 4,得剩余序列的周期为 2:1,3, …;对式(30)取模 4,得剩余序列的周期为 2:0,2, …。此时,式(28)成为 $y^2\equiv 3(\bmod 4)$, 不可能。

当 $u_1\equiv 1(\bmod 8),v_1\equiv 4(\bmod 8)$ 时, 对式(29)取模 8,得剩余序列的周期为 1:1,1, …;对式(30)取模 8,得剩余序列的周期为 2:0,4, …。此时,式(28)成为 $y^2\equiv 7,3(\bmod 8)$, 不可能。

当 $u_1\equiv 5(\bmod 8),v_1\equiv 4(\bmod 8)$ 时, 对式(29)取模 8,得剩余序列的周期为 2:1,5, …;对式(30)取模 8,得剩余序列的周期为 2:0,4, …。

此时式(28)成为 $y^2 \equiv 7 \pmod 8$, 不可能。

当 $u_1 \equiv 7 \pmod 8$, $v_1 \equiv 4 \pmod 8$ 时,对式(29)取模 8,得剩余序列的周期为 2:1,7,…;对式(30)取模 8,得剩余序列的周期为 2:0,4,…。此时,式(28)成为 $y^2 \equiv 7,5 \pmod 8$, 不可能。

当 $u_1 \not\equiv 7 \pmod 8$, $v_1 \equiv 0 \pmod 8$ 时,式(28)成为 $y^2 \equiv 3,5,7 \pmod 8$, 也不可能。

证毕。

4 推论的证明

先证推论 1。若 $2 \mid y$, 则有 $4 \mid x$。令 $x = 4x_1$, $y = 2y_1$, 则式(3)可化为

$$x_1^2 - 33y_1^4 = 1 \tag{31}$$

根据引理 5,式(31)给出 $x_1 = 23, y_1 = 2$。此时可得式(3)的解为 $(x,y) = (92,4)$。

若 $2 \nmid y$, 则 $\gcd(x,y) = 1$。因为 $23 + 4\sqrt{33}$ 为 Pell 方程 $U^2 - 33V^2 = 1$ 的基本解,根据引理 1,方程 $X^2 - 33Y^2 = 16$ 的最小正整数解 $X_1 + Y_1\sqrt{33}$ 中 Y_1 满足 $0 < Y_1 \leqslant \dfrac{4\sqrt{16}}{\sqrt{2 \times 24}} < 2.4$。经计算,仅有 $X_1 = 7, Y_1 = 1$, 故该方程的解仅有 2 个非结合类。又 $23 \equiv 7 \pmod 8$, $4 \equiv 4 \pmod 8$, $p = 3, m = 3$, 所以由定理知,式(3)适合 $\gcd(x,y) = 1$ 的解必满足

$$y^2 = u_n + 7v_n,\ n \geqslant 0 \tag{32}$$

根据引理 3,有

$$u_{n+2} = 46u_{n+1} - u_n, u_0 = 1, u_1 = 23 \tag{33}$$

$$v_{n+2} = 46v_{n+1} - v_n, v_0 = 0, v_1 = 4 \tag{34}$$

$$u_{2n} = u_n^2 + 33v_n^2 = 2u_n^2 - 1 = 66v_n^2 + 1$$

$$v_{2n} = 2u_nv_n \tag{35}$$

$$u_{3n} = u_n(u_n^2 + 99v_n^2) \tag{36}$$

$$u_{-n} = u_n, v_{-n} = -v_n \tag{37}$$

$$u_{n+2km} \equiv (-1)^k u_n \pmod{u_m}$$

$$v_{n+2km} \equiv (-1)^k v_n \pmod{u_m} \tag{38}$$

约定:下文中“T”表示取模所得剩余序列的周期。

利用式(33)和式(34),对式(32)取模 151,得 $T = 8$, 且当 $n \equiv 1,4,6,7 \pmod 8$ 时, $y^2 \equiv 51, 150, 71, 146 \pmod{151}$ 均为模 151 的平方非剩余,故排除,剩 $n \equiv 0,2,3,5 \pmod 8$。

对式(32)取模 7,得 $T = 8$, 且当 $n \equiv 3,5 \pmod 8$ 时, $y^2 \equiv 5 \pmod 7$ 为模 7 的平方非剩余,故排除,剩 $n \equiv 0,2 \pmod 8$, 即 $n \equiv 0,2,8,10,16,18 \pmod{24}$。

对式(32)取模 433, 得 $T = 24$, 且当 $n \equiv 2,8,10 \pmod{24}$ 时, $y^2 \equiv 180, 344, 231 \pmod{433}$ 均为模 433 的平方非剩余,故排除,剩 $n \equiv 0,16,18 \pmod{24}$。

对式(32)取模 1 153,得 $T = 48$, 且当 $n \equiv 16, 40 \pmod{48}$ 时, $y^2 \equiv 964, 189 \pmod{1\,153}$ 均为模 1 153 的平方非剩余,故排除 $n \equiv 16 \pmod{24}$, 剩 $n \equiv 0,18 \pmod{24}$, 故 $n \equiv 0 \pmod 6$。

若 $n \neq 0$, 可设 $n = 2 \times 3^t(3k \pm 1)$ ($t \geqslant 1$), 并取 $m = 3^t$, 则 $m \equiv 3 \pmod 6$。

利用式(37)和式(38),可将式(32)化为

$$y^2 \equiv \pm(u_{\pm 2m} + 7v_{\pm 2m}) \equiv \pm(u_{2m} \pm 7v_{2m}) \pmod{u_{3m}}$$

由式(36)知, $u_{3m} = u_m(u_m^2 + 99v_m^2)$, 故有

$$y^2 \equiv \pm(u_{2m} \pm 7v_{2m}) \pmod{u_m^2 + 99v_m^2} \tag{39}$$

考虑到 $u_m^2 + 99v_m^2 \equiv 1 \pmod 8$, $u_m \equiv 1 \pmod{11}$, 且当 $m \equiv 3 \pmod 6$ 时, $u_m \equiv 2 \pmod 3$, $7u_m \pm 33v_m \equiv 1 \pmod 4$, $7u_m \pm 33v_m \equiv 3 \pmod 5$, 故由式(39)结合式(35)可得

$$\begin{aligned}
1 &= \left(\frac{y^2}{u_m^2 + 99v_m^2}\right) = \left(\frac{\pm(u_{2m} \pm 7v_{2m})}{u_m^2 + 99v_m^2}\right) \\
&= \left(\frac{u_{2m} \pm 7v_{2m}}{u_m^2 + 99v_m^2}\right) = \left(\frac{u_m^2 + 33v_m^2 \pm 14u_mv_m}{u_m^2 + 99v_m^2}\right) \\
&= \left(\frac{-66v_m^2 \pm 14u_mv_m}{u_m^2 + 99v_m^2}\right) \\
&= \left(\frac{\pm 2v_m}{u_m^2 + 99v_m^2}\right)\left(\frac{7u_m \mp 33v_m}{u_m^2 + 99v_m^2}\right) \\
&= \left(\frac{u_m^2 + 99v_m^2}{7u_m \mp 33v_m}\right) = \left(\frac{49u_m^2 + 4851v_m^2}{7u_m \mp 33v_m}\right) \\
&= \left(\frac{5940v_m^2}{7u_m \mp 33v_m}\right) = \left(\frac{2^2 \times 3^3 \times 5 \times 11v_m^2}{7u_m \mp 33v_m}\right) \\
&= \left(\frac{3}{7u_m \mp 33v_m}\right)\left(\frac{5}{7u_m \mp 33v_m}\right)\left(\frac{11}{7u_m \mp 33v_m}\right) \\
&= \left(\frac{7u_m \mp 33v_m}{3}\right)\left(\frac{7u_m \mp 33v_m}{5}\right)\left(\frac{7u_m \mp 33v_m}{11}\right) \\
&= \left(\frac{7}{3}\right)\left(\frac{2}{3}\right)\left(\frac{3}{5}\right)\left(\frac{7}{11}\right) = -1
\end{aligned}$$

矛盾。因此 $n = 0$。代入式(32),得 $y = 1$。此时可得式(3)的解 $(x,y) = (7,1)$。

综上,方程(3) 仅有解 $(x,y) = (7,1)$ 和 $(92,4)$。证毕。

再证推论 2。若 $2 \mid y$, 则有 $4 \mid x$。令 $x = 4x_1$, $y = 2y_1$, 则式(4)可化为

$$x_1^2 - 209y_1^4 = 1 \tag{40}$$

根据引理 10,式(40)无正整数解,故此时式(4)

无解。

若 $2 \nmid y$, 则 $\gcd(x,y) = 1$。因为 $46\,551 + 3\,220 \times \sqrt{209}$ 为 Pell 方程 $U^2 - 209V^2 = 1$ 的基本解,根据引理 1,方程 $X^2 - 209Y^2 = 16$ 的最小正整数解 $X_1 + Y_1\sqrt{33}$ 中 Y_1 满足 $0 < Y_1 \leqslant \dfrac{3\,220\sqrt{16}}{\sqrt{2 \times 46\,552}} < 42.3$。经计算,仅有 $X_1 = 15, Y_1 = 1$, 故该方程的解仅有 2 个非结合类。又 $46\,551 \equiv 7 \pmod 8$, $3\,220 \equiv 4 \pmod 8$, $p = 11, m = 3$, 所以由定理知,式(4)适合 $\gcd(x,y) = 1$ 的解必满足

$$y^2 = u_n + 15v_n, n \geqslant 0 \tag{41}$$

根据引理 3,有

$$u_{n+2} = 93\,102u_{n+1} - u_n, u_0 = 1, u_1 = 46\,551 \tag{42}$$

$$v_{n+2} = 93\,102v_{n+1} - v_n, v_0 = 0, v_1 = 3\,220 \tag{43}$$

$$u_{2n} = u_n^2 + 209v_n^2 = 2u_n^2 - 1 = 418v_n^2 + 1$$
$$v_{2n} = 2u_nv_n \tag{44}$$

$$u_{n+2km} \equiv (-1)^k u_n \pmod{u_m}$$
$$v_{n+2km} \equiv (-1)^k v_n \pmod{u_m} \tag{45}$$

利用式(42)和式(43),对式(41)取模 59,得 $T = 4$, 且当 $n \equiv 1,2 \pmod 4$ 时, $y^2 \equiv 38,58 \pmod{59}$ 均为模 59 的平方非剩余,故排除,剩 $n \equiv 0,3 \pmod 4$, 即 $n \equiv 0,3,4,7,8,11,12,15,16,19 \pmod{20}$。

对式(41)取模 41,得 $T = 40$, 且当 $n \equiv 3,23,8,28,12,32,16,36,19,39 \pmod{40}$ 时, $y^2 \equiv 14,27,12,29,6,35,30,11,27,14 \pmod{41}$ 均为模 41 的平方非剩余,故排除,剩 $n \equiv 0,4,7,11,15 \pmod{20}$。

对式(41)取模 281,得 $T = 40$, 且当 $n \equiv 7,27,11,31,15,35 \pmod{40}$ 时, $y^2 \equiv 21,260,104,177,278,3 \pmod{281}$ 均为模 281 的平方非剩余,故排除 $n \equiv 7,11,15 \pmod{20}$, 剩 $n \equiv 0,4 \pmod{20}$。

对式(41)取模 601,得 $T = 40$, 且当 $n \equiv 4,24 \pmod{40}$ 时, $y^2 \equiv 7,594 \pmod{601}$ 均为模 601 的平方非剩余, 故排除 $n \equiv 4 \pmod{20}$, 剩 $n \equiv 0 \pmod{20}$。

若 $n \neq 0$, 可设 $n = 2 \times 5 \times 2^t(2k+1)$ ($t \geqslant 1$, $k \geqslant 0$),并取 $m = \begin{cases} 2^t, & t \equiv 0 \pmod 2 \\ 5 \times 2^t, & t \equiv 1 \pmod 2 \end{cases}$, 则 $m \equiv 1 \pmod 3$, 从而 $2m \equiv 2 \pmod 3$。

利用式(45),可将式(41)化为

$$y^2 \equiv \pm(u_{2m} + 15v_{2m}) \equiv \pm 15v_{2m} \pmod{u_{2m}} \tag{46}$$

考虑到 $2 \mid m$ 时, $u_m \equiv 1 \pmod 8, u_{2m} \equiv 1 \pmod 8$。令 $2^s \parallel v_m$, 结合式(44),则式(46)可化为

$$\begin{aligned} 1 &= \left(\frac{y^2}{u_{2m}}\right) = \left(\frac{\pm 15v_{2m}}{u_{2m}}\right) \\ &= \left(\frac{15}{u_{2m}}\right)\left(\frac{2}{u_{2m}}\right)\left(\frac{u_m}{u_{2m}}\right)\left(\frac{v_m}{u_{2m}}\right) \\ &= \left(\frac{u_{2m}}{15}\right)\left(\frac{2u_m^2 - 1}{u_m}\right)\left(\frac{418v_m^2 + 1}{v_m/2^s}\right) \\ &= \left(\frac{u_{2m}}{15}\right) \end{aligned} \tag{47}$$

由于 $\{u_n\}$ 取模 15 的 $T = 3$, 且当 $2m \equiv 2 \pmod 3$ 时, $u_{2m} \equiv 11 \pmod{15}$, 故式(47)给出 $1 = \left(\dfrac{11}{15}\right) = -1$, 矛盾。因此 $n = 0$。代入式(41)得 $y = 1$。此时可得式(4)的解 $(x,y) = (15,1)$。

综上, 方程(4)仅有解 $(x,y) = (15,1)$。证毕。

最后证推论 3。若 $2 \mid y$, 则有 $4 \mid x$。令 $x = 4x_1$, $y = 2y_1$, 则式(5)可化为

$$x_1^2 - 65y_1^4 = 1 \tag{48}$$

根据引理 6,式(48)给出 $x_1 = 129, y_1 = 4$。此时可得式(5)的解为 $(x,y) = (516,8)$。

若 $2 \nmid y$, 则 $\gcd(x,y) = 1$。因为 $129 + 16\sqrt{65}$ 为 Pell 方程 $U^2 - 65V^2 = 1$ 的基本解,根据引理 1, 方程 $X^2 - 65Y^2 = 16$ 的最小正整数解 $X_1 + Y_1\sqrt{33}$ 中 Y_1 满足 $0 < Y_1 \leqslant \dfrac{16\sqrt{16}}{\sqrt{2 \times 130}} < 3.97$。经计算,仅有 $X_1 = 9, Y_1 = 1$, 故该方程的解仅有 2 个非结合类。又 $129 \equiv 1 \pmod 8$, $16 \equiv 0 \pmod 8$, $p = 5$, $m = 3$, 所以由定理知,式(5)适合 $\gcd(x,y) = 1$ 的解必满足

$$y^2 = u_n + 9v_n, n \geqslant 0 \tag{49}$$

根据引理 3,有

$$u_{n+2} = 258u_{n+1} - u_n, u_0 = 1, u_1 = 129 \tag{50}$$

$$v_{n+2} = 258v_{n+1} - v_n, v_0 = 0, v_1 = 16 \tag{51}$$

$$u_{2n} = u_n^2 + 65v_n^2 = 2u_n^2 - 1 = 130v_n^2 + 1$$
$$v_{2n} = 2u_nv_n \tag{52}$$

$$u_{3n} = u_n(u_n^2 + 195v_n^2) \tag{53}$$

$$u_{-n} = u_n, v_{-n} = -v_n \tag{54}$$

$$u_{n+2km} \equiv (-1)^k u_n \pmod{u_m}$$
$$v_{n+2km} \equiv (-1)^k v_n \pmod{u_m} \tag{55}$$

利用式(50)和式(51),对式(49)取模 29,得 $T = 14$,且当 $n \equiv 1,2,3,5,6,8,9,10,12,13 \pmod{14}$ 时,$y^2 \equiv 12,21,12,14,15,17,8,17,15,14 \pmod{29}$ 均为模 29 的平方非剩余,故排除,剩 $n \equiv 0,4,7,11 \pmod{14}$,即 $n \equiv 0,4,7,11,14,18,21,25 \pmod{28}$。

对式(49)取模 43,得 $T = 4$,且当 $n \equiv 2,3 \pmod 4$ 时,$y^2 \equiv 42,28 \pmod{43}$ 均为模 43 的平方非剩余,故排除 $n \equiv 7,11,14,18 \pmod{28}$,剩 $n \equiv 0,4,21,25 \pmod{28}$,即 $n \equiv 0,4,21,25,28,32,49,53 \pmod{56}$。

对式(49)取模 503,得 $T = 56$,且当 $n \equiv 25,28,32,49 \pmod{56}$ 时,$y^2 \equiv 248,502,358,93 \pmod{503}$ 均为模 503 的平方非剩余,故排除,剩 $n \equiv 0,4,21,53 \pmod{56}$。

对式(49)取模 4 817,得 $T = 56$,且当 $n \equiv 4,21,53 \pmod{56}$ 时,$y^2 \equiv 1\,644,3\,726,3\,233 \pmod{4\,817}$ 均为模 4 817 的平方非剩余,故排除,剩 $n \equiv 0 \pmod{56}$,从而 $n \equiv 0 \pmod{14}$。

对式(49)取模 37,得 $T = 3$,且当 $n \equiv 1,2 \pmod 3$ 时,$y^2 \equiv 14,22 \pmod{37}$ 均为模 37 的平方非剩余,故排除,剩 $n \equiv 0 \pmod 3$。结合 $n \equiv 0 \pmod{14}$,可得 $n \equiv 0 \pmod{42}$。

若 $n \neq 0$,可设 $n = 2 \times 7 \times 3^t \times k$($t \geqslant 1, 3 \nmid k > 0$),并选择 $m = 3^t$ 或 7×3^t。对 k 分两种情况讨论。

(ⅰ)$k \equiv 1 \pmod 3$ 时,令

$$m = \begin{cases} 3^t, & t \equiv 1 \pmod 2 \\ 7 \times 3^t, & t \equiv 0 \pmod 2 \end{cases}$$

则 $m \equiv 3 \pmod{12}$。

利用式(55),可将式(49)化为

$$y^2 \equiv \pm (u_{2m} + 9v_{2m}) \pmod{u_{3m}}$$

由式(53)知,$u_{3m} = u_m(u_m^2 + 195v_m^2)$,故有

$$y^2 \equiv \pm (u_{2m} + 9v_{2m}) \pmod{u_m^2 + 195v_m^2} \quad (56)$$

由式(50)和式(51)知,$u_m^2 + 195v_m^2 \equiv 1 \pmod 8$,$9u_m - 65v_m \equiv 4,1 \pmod 5$,$9u_m - 65v_m \equiv 9,4 \pmod{13}$。利用式(52),则式(56)给出

$$\begin{aligned} 1 &= \left(\frac{y^2}{u_m^2 + 195v_m^2}\right) = \left(\frac{\pm (u_{2m} + 9v_{2m})}{u_m^2 + 195v_m^2}\right) \\ &= \left(\frac{u_m^2 + 65v_m^2 + 18u_m v_m}{u_m^2 + 195v_m^2}\right) \\ &= \left(\frac{-130v_m^2 + 18u_m v_m}{u_m^2 + 195v_m^2}\right) \\ &= \left(\frac{2v_m}{u_m^2 + 195v_m^2}\right)\left(\frac{9u_m - 65v_m}{u_m^2 + 195v_m^2}\right) \\ &= \left(\frac{u_m^2 + 195v_m^2}{9u_m - 65v_m}\right) = \left(\frac{81u_m^2 + 15795v_m^2}{9u_m - 65v_m}\right) \\ &= \left(\frac{20020v_m^2}{9u_m - 65v_m}\right) = \left(\frac{2^2 \times 5 \times 13 \times 77v_m^2}{9u_m - 65v_m}\right) \\ &= \left(\frac{9u_m - 65v_m}{5}\right)\left(\frac{9u_m - 65v_m}{13}\right)\left(\frac{9u_m - 65v_m}{77}\right) \\ &= \left(\frac{9u_m - 65v_m}{77}\right) \end{aligned} \quad (57)$$

由于 $\{9u_n - 65v_n\}$ 取模 77 的 $T = 12$,且当 $m \equiv 3 \pmod{12}$ 时,$9u_m - 65v_m \equiv 65 \pmod{77}$,故式(57)给出 $1 = \left(\frac{65}{77}\right) = -1$,矛盾。

(ⅱ)$k \equiv -1 \pmod 3$ 时,令

$$m = \begin{cases} 3^t, & t \equiv 0 \pmod 2 \\ 7 \times 3^t, & t \equiv 1 \pmod 2 \end{cases}$$

则 $m \equiv 9 \pmod{12}$。

利用式(54)和式(55),可将式(49)化为

$$y^2 \equiv \pm (u_{2m} - 9v_{2m}) \pmod{u_{3m}} \quad (58)$$

由式(53)知,$u_{3m} = u_m(u_m^2 + 195v_m^2)$,故由式(58)可得

$$y^2 \equiv \pm (u_{2m} - 9v_{2m}) \pmod{u_m^2 + 195v_m^2} \quad (59)$$

由式(50)和式(51)知,$u_m^2 + 195v_m^2 \equiv 1 \pmod 8$,$9u_m + 65v_m \equiv 4,1 \pmod 5$,$9u_m + 65v_m \equiv 9,4 \pmod{13}$。完全类似式(56)的讨论知,式(59)给出

$$1 = \left(\frac{9u_m + 65v_m}{77}\right) \quad (60)$$

由于 $\{9u_n + 65v_n\}$ 取模 77 的 $T = 12$,且当 $m \equiv 9 \pmod{12}$ 时,$9u_m + 65v_m \equiv 65 \pmod{77}$,故式(60)给出 $1 = \left(\frac{65}{77}\right) = -1$,矛盾。

因此 $n = 0$。代入式(49)得 $y = 1$。此时可得式(5)的解 $(x,y) = (9,1)$。

综上,方程(5)仅有解 $(x,y) = (9,1)$ 和 $(516,8)$。证毕。

参考文献:

[1] 管训贵. 椭圆曲线在 $y^2 = x(x-p)(x-q)$ 的整数点(I)[J]. 数学的实践与认识, 2018, 48(4): 272-279.

[2] 管训贵. 椭圆曲线在 $y^2 = x(x-p)(x-q)$ 的整数点(II)[J]. 安徽大学学报(自然科学版), 2018, 42(2): 41-46.

[3] 冉银霞. 椭圆曲线在 $y^2 = x(x+p)(x+q)$ 的整数点[J]. 南宁师范大学学报(自然科学版), 2021, 38(1): 54-59.

[4] 管训贵. 初等数论[M]. 2 版. 合肥: 中国科学技术大学出版社, 2016: 247-248.

(下转第 42 页)