A NOTE ON THE DIOPHANTINE EQUATION $x^{2p} - Dy^2 = 1$

LE MAOHUA

(Communicated by William W. Adams)

Abstract. Let $D$ be a positive integer which is square free, and let $p$ be a prime. In this note we prove that if $p = 2$ and $D > \exp 64$, then the equation $x^{2p} - Dy^2 = 1$ has at most one positive integer solution $(x,y)$; if $p > 2$ and $D > \exp \exp \exp \exp 10$, then every positive integer solution $(x,y)$ can be expressed as $x^p + y\sqrt{D} = \varepsilon_1^m$, where $m$ is a positive integer with $2 \nmid m$, $\varepsilon_1$ is the fundamental solution of Pell's equation $u^2 - Dv^2 = 1$.

I. Introduction

Let $D$ be a positive integer which is square free, $\varepsilon_1 = u_1 + v_1\sqrt{D}$ be the fundamental solution of the equation

$$u^2 - Dv^2 = 1,$$

and let $p$ be a prime. In 1942, Ljunggren [8] showed that if $p = 2$ then the equation

$$x^{2p} - Dy^2 = 1$$

has at most two positive integer solutions. The author [5] proved that if $p = 2$ then (2) has positive integer solution $(x,y)$ if and only if either $u_1$ or $u_1^2 + Dv_1^2$ is a square. In this note we prove:

Theorem 1. If $p = 2$ and $D > \exp 64$, then (2) has at most one positive integer solution $(x,y)$.

Clearly, every solution $(x,y)$ of (2) can be expressed as

$$x^p + y\sqrt{D} = \varepsilon_1^m,$$

where $m$ is a positive integer. Recently, Cao [3] showed that if $p > 2$ then $4 \nmid m$. We prove:

Theorem 2. If $p > 2$ and $D > \exp \exp \exp \exp 10$, then $2 \nmid m$.  □
2. Proof of Theorem 1

Lemma 1 [7, Formula 1.76]. Let \( n \) be a positive integer and let \( \alpha, \beta \) be complex numbers. Then

\[
\alpha^n + \beta^n = \sum_{i=0}^{[n/2]} (-1)^i \binom{n}{i} (\alpha + \beta)^{n-2i} (\alpha \beta)^i,
\]

where

\[
\binom{n}{i} \frac{(n-i-1)!n}{(n-2i)!i!}, \quad i = 0, \ldots, \binom{n}{2}
\]

are positive integers. \( \Box \)

Lemma 2. Let \( d \) be a positive integer which is nonsquare. If \((U, V)\) is a positive integer solution of

\[
U^2 - dV^2 = \lambda, \quad \lambda = \pm1,
\]

then every positive integer solution \((U', V')\) of \( (4) \) such that \( U | U' \) can be expressed as

\[
U' + V'\sqrt{d} = (U + V\sqrt{d})^t,
\]

where \( t \) is a positive integer with \( 2 \nmid t \).

Proof. Clearly, if \( U', V' \) satisfy \( (5) \), then \((U', V')\) is a positive integer solution of \( (4) \) with \( U | U' \). On the other hand, if \((U, V)\) and \((U', V')\) are positive integer solutions of \( (4) \) with \( U \leq U' \), then there exist positive integers \( s_1, s_2 \) such that

\[
U = \frac{\rho^{s_1} + \bar{\rho}^{s_1}}{2}, \quad U' = \frac{\rho^{s_2} + \bar{\rho}^{s_2}}{2}, \quad s_1 \leq s_2,
\]

where \( \rho = U + V\sqrt{d} \) is the fundamental solution of \( (4) \). If \( s_1 = s_2 \), then \( t = 1 \) and the lemma holds. If \( s_1 < s_2 \), then there exist integers \( a, b \) such that \( s_2 = 2as_1 \pm b, \ a > 0, \ 0 < b \leq s_1 \). From

\[
\frac{\rho^{s_2} + \bar{\rho}^{s_2}}{2} + (\rho\bar{\rho})^{s_1} \frac{\rho^{s_2-2s_1} + \bar{\rho}^{s_2-2s_1}}{2} = 2 \left( \frac{\rho^{s_1} + \bar{\rho}^{s_1}}{2} \right) \left( \frac{\rho^{s_2-3s_1} + \bar{\rho}^{s_2-3s_1}}{2} \right),
\]

we see that if \( U | U' \) then

\[
U' \equiv \left| \frac{\rho^{s_1} + \bar{\rho}^{s_1}}{2} \right| \equiv \left| \frac{\rho^{s_2-2s_1} + \bar{\rho}^{s_2-2s_1}}{2} \right| \equiv \cdots \equiv \left| \frac{\rho^{s_2-2as_1} + \bar{\rho}^{s_2-2as_1}}{2} \right| \equiv \left| \frac{\rho^b + \bar{\rho}^b}{2} \right| \equiv 0 \pmod{U}.
\]

Since, if \( b < s_1 \) then \( 0 < \frac{1}{2}(\rho^b + \bar{\rho}^b) < \frac{1}{2}(\rho^{s_1} + \bar{\rho}^{s_1}) = U \). It follows that \( b = s_1 \) and \( s_2 = (2a \pm 1)s_1 \). Hence the lemma. \( \Box \)
Lemma 3. If \((u, v)\) and \((u', v')\) are positive integer solutions of (1) with \(u|u'\), then there exist fixed positive integers \(D_1, D_2\) such that \(D_1D_2 = D\),

\[
\begin{align*}
\delta &= \begin{cases} 
1, & 2|u, \\
2, & 2 \nmid u,
\end{cases} \\
\delta &v_1v_2 = v, \delta v'_1v'_2 = v',
\end{align*}
\]

where \(\delta, v_1, v_2, v_1', v_2'\) are positive integers satisfy

\[
\begin{align*}
\delta &= \begin{cases} 
1, & 2|u, \\
2, & 2 \nmid u,
\end{cases} \\
\delta &v_1v_2 = v, \delta v'_1v'_2 = v'.
\end{align*}
\]

Proof. Since \(D\) is square free, from (1) we get (6) clearly. Let \(\eta = v_1\sqrt{D_1} + v_2\sqrt{D_2}, \bar{\eta} = v_1\sqrt{D_1} - v_2\sqrt{D_2},\) then \(\eta + \bar{\eta} = 2v_1\sqrt{D_1}, \eta - \bar{\eta} = 2v_2\sqrt{D_2}, \eta\bar{\eta} = 2/\delta\). Further let \(e = u + v\sqrt{D}, \bar{e} = u - v\sqrt{D},\) then \(e = (\delta/2)\eta^2, \bar{e} = (\delta/2)\bar{\eta}^2\). By Lemma 2, if \(u|u'\) then

\[
\begin{align*}
u' + v'\sqrt{D} &= e', \\
u' - v'\sqrt{D} &= \bar{e'},
\end{align*}
\]

\(t > 0, 2 \nmid t\). Clearly, by (6), the lemma holds when \(t = 1\). If \(t > 1\), by Lemma 1, then we have

\[
\begin{align*}
u' + 1 &= \frac{e' + \bar{e}'}{2} + 1 = \frac{1}{2} \left( \frac{\delta}{\delta_2^2} \right)^t + \left( \frac{\delta}{\delta_2^2} \right)^t + 2 = \frac{1}{2} \left( \frac{\delta}{\delta_2^2} \right)^t (\eta' + \bar{\eta}')^2 \\
u' - 1 &= \delta D_2 v_2^2 \left( \sum_{i=0}^{t-1/2} \left( \frac{t}{i} \right) (2\delta D_1 v_1^2)^{(t-1/2-i)} \right)
\end{align*}
\]

and

\[
\begin{align*}
u' - 1 &= \delta D_2 v_2^2 \left( \sum_{i=0}^{t-1/2} \left( \frac{t}{i} \right) (2\delta D_2 v_2^2)^{(t-1/2-i)} \right)
\end{align*}
\]

The lemma is proved. \(\square\)

Lemma 4 [4, Theorem 2]. If \(p = 2\), then \(m \mod (3)\) satisfies \(4 \nmid m\). \(\square\)

Lemma 5 [5, Proof of Theorem]. If \((u, v)\) is a positive integer solution of (1), \(e = u + v\sqrt{D}, \bar{e} = u - v\sqrt{D},\) then for any odd prime \(q\) and integer \(z\), \((e^q + \bar{e}^q)/(e + \bar{e}) = qz^2\) is impossible. \(\square\)

Lemma 6 [10]. Let \(\beta, \alpha_1, \alpha_2\) be nonzero algebraic numbers with degrees \(D_0, D_1, D_2\) and heights \(H_0, H_1, H_2\), respectively, \(B = \max(\alpha_0, H_0), A_j = \max(\log \alpha_j, H_j) (j = 1, 2),\) and let \(D\) denote the degree of the field \(\mathbb{Q}(\beta, \alpha_1, \alpha_2).\) If \(\Lambda = \beta \log \alpha_1 - \log \alpha_2 \neq 0,\) then

\[
|\Lambda| > \exp \left( -5 \cdot 10^8 D^4 \frac{S_1 S_2}{D_1 D_2} T^2 (\log E)^{-3} \right),
\]

where \(S_0 = D_0 + \log B, S_j = D_j + \log A_j (j = 1, 2), T = 4 + \frac{S_0}{D_0} + \log \left( \frac{D^2 S_1 S_2}{D_1 D_2} \right), E > e.\)
Proof of Theorem 1. When \( p = 2 \), if (2) has two positive integer solutions \((x_1, y_1)\) and \((x_2, y_2)\) with \(x_1 < x_2\), then there exist integers \(s_1, s_2\) such that

\[
x_1^2 = \frac{\varepsilon_1^{s_1} + \varepsilon_1^{s_2}}{2}, \quad x_2^2 = \frac{\varepsilon_1^{s_2} + \varepsilon_1^{s_1}}{2}, \quad 0 < s_1 < s_2,
\]

where \(\varepsilon_1 = u_1 - v_1 \sqrt{D}\). Write \(s_2 = 2's'\), \(r \geq 0\), \(2 \nmid s'\). By Lemma 4, if \(s' = 1\) then \(r = 1\), thereby \(s_1 = 1\), \(s_2 = 2\), and \(x_2^2 - 2x_1^2 = -1\), \(x_2 > 1\), \(x_1 > 1\). By [9], we see that \((x_1, x_2) = (13, 239)\) and \(D = 1785\). It follows that if \(D \neq 1785\), then \(s' > 1\) and \(s'\) has an odd prime factor \(q\). Put \(\varepsilon = \varepsilon_1^{s_2/q}\), \(\overline{\varepsilon} = \varepsilon_1^{s_1/q}\), then \(\varepsilon = u + v\sqrt{D}\), \(\overline{\varepsilon} = u - v\sqrt{D}\), where \((u, v)\) is a positive integer solution of (1). By Lemma 1, from (7) we get

\[
x_2^2 = \frac{\varepsilon^{s_2} + \overline{\varepsilon}^{s_2}}{2} = \left(\frac{\varepsilon + \overline{\varepsilon}}{2}\right) \left(\frac{\varepsilon^{s_2} + \overline{\varepsilon}^{s_2}}{\varepsilon + \overline{\varepsilon}}\right) = \left(\frac{\varepsilon^{s_2} + \overline{\varepsilon}^{s_2}}{\varepsilon + \overline{\varepsilon}}\right).
\]

Since

\[
\frac{\varepsilon^{s_2} + \overline{\varepsilon}^{s_2}}{\varepsilon + \overline{\varepsilon}} = \sum_{i=0}^{(q-1)/2} (-1)^i \left[\frac{q}{i}\right] (2u)^{q-2i-1} \equiv (-1)^{(q-1)/2} q \pmod{u},
\]

from (8) we obtain

\[
(9) \quad u = cx_2^2, \quad \frac{\varepsilon^{s_2} + \overline{\varepsilon}^{s_2}}{\varepsilon + \overline{\varepsilon}} = cx_2^2, \quad c = 1 \text{ or } q, \quad cx_2^i x_2^2 = x_2.
\]

Further, by Lemma 5, (9) is impossible when \(c = q\). Therefore \(c = 1\) and \(u = x_2^2\). Note that (2) has at most two solutions when \(p = 2\). We see that \(x_2^i = x_1\) and \(x_1 | x_2\). Then, by Lemma 3, we have

\[
(10) \quad x_1^2 + 1 = \delta D_1 y_{11}^2, \quad x_1^2 - 1 = \delta D_2 y_{12}^2,
\]

\[
(11) \quad x_2^2 + 1 = \delta D_1 y_{21}^2, \quad x_2^2 - 1 = \delta D_2 y_{22}^2,
\]

where

\[
\delta = \{1, 2\} x_1, \quad D_1 D_2 = D, \quad \delta y_{11} y_{12} = y_1, \quad \delta y_{21} y_{22} = y_2.
\]

Let \(\rho_1 = x_1 + y_{11} \sqrt{D_1}, \quad \overline{\rho}_1 = x_1 - y_{11} \sqrt{D_1}, \quad \rho_2 = x_1 + y_{12} \sqrt{D_2}, \quad \overline{\rho}_2 = x_1 - y_{12} \sqrt{D_2}\). Since \(x_1 < x_2\) and \(x_1 | x_2\), by Lemma 2, from (10) and (11) we obtain

\[
x_2 + y_{21} \sqrt{D_1} = \rho_1^{t_1}, \quad x_2 - y_{21} \sqrt{D_1} = \overline{\rho}_1^{t_1}, \quad t_1 > 1, \quad 2 \nmid t_1,
\]

\[
x_2 + y_{22} \sqrt{D_2} = \rho_2^{t_2}, \quad x_2 - y_{22} \sqrt{D_2} = \overline{\rho}_2^{t_2}, \quad t_2 > 1, \quad 2 \nmid t_2.
\]

Hence

\[
(12) \quad \rho_1 + \overline{\rho}_1 = \rho_2 + \overline{\rho}_2,
\]

\[
(13) \quad \rho_1^{t_1} + \overline{\rho}_1^{t_1} = \rho_2^{t_2} + \overline{\rho}_2^{t_2}.
\]
A NOTE ON THE DIOPHANTINE EQUATION $x^{2\sigma} - d y^2 = 1$

Since $\rho_1 \bar{\rho}_1 = -1$, $\rho_1 > 0$, $\bar{\rho}_1 < 0$, $\rho_2 \bar{\rho}_2 = 1$, $\rho_2 > 0$, $\bar{\rho}_2 > 0$. From (12), (13) we get $\rho_1 > \rho_2$,

(14) \hspace{1cm} t_1 < t_2,
(15) \hspace{1cm} \log \rho_1 = \log \rho_2 + \Delta_1,
(16) \hspace{1cm} t_1 \log \rho_1 = t_2 \log \rho_2 + \Delta_2,

where

\[ 0 < \Delta_1 = \frac{2}{\rho_1 \rho_2} \sum_{l=0}^{\infty} \frac{(\rho_1 \rho_2)^{-2l}}{2l + 1} < \frac{4}{\rho_1^2}, \quad 0 < \Delta_2 = \frac{2}{\rho_1 \rho_2} \sum_{l=0}^{\infty} \frac{(\rho_1 \rho_2)^{-2l}}{2l + 1} < \frac{4}{\rho_2^2}. \]

From (15), (16) we get

(17) \hspace{1cm} t_2 = \frac{(t_2 - t_1) \log \rho_1 + \Delta_2}{\Delta_1} > \frac{\rho_1^2}{2 \log \rho_1}.

On the other hand, since $\rho_1^2 - 2x_1 \rho_1 - 1 = 0$ and $\rho_2^2 - 2x_2 \rho_2 + 1 = 0$, we see from Lemma 6 and (14) that

\[ \left| \frac{t_1}{t_2} \log \rho_1 - \log \rho_2 \right| > \exp \left( -5 \cdot 10^8 D^4 \frac{S_1 S_2}{D_1 D_2} T^2 (\log E)^{-3} \right), \]

where $D_0 = 1$, $D = 2$, $D_2 = 2$, $D = 4$, $H_0 = t_2$, $H_1 = 2x_1$, $H_2 = 2x_1$, $B = t_2$, $A_1 = \rho_1$, $A_2 < \rho_1$, $S_0 = 1 + \log t_2$, $S_1 = 2 + \log \rho_1$, $s_2 < 2 + \log \rho_1$, $T < 5 + \log t_2 + \log(4(2 + \log \rho_1)^2)$, $E > e$. On combining this with (16) we obtain

(18) \hspace{1cm} \log 4 + 4^3 \cdot 5 \cdot 10^8 (2 + \log \rho_1)^2 (5 + \log t_2 + \log(4(2 + \log \rho_1)^2))^2 > \log t_2 + 2t_2 \log \rho_2.

Since $\log \log \log \rho_1 < \log \log \rho_1$, $\log(2 + \log \rho_1) < 2 \log \log \rho_1$, $\rho_1 < \rho_2^{15}$, and $\log \log \rho_1 > \log \log x_1 > \log \log D^{1/4} > 1$ when $D > \exp 64$. Then from (18) we conclude

\[ t_2 < e^{29 \log \rho_1 (\log \log \rho_1)^2}. \]

Substitute it into (17) we deduce

\[ 2e^{29 (\log \log \rho_1)^2} > \rho_1^2, \]

whence $\rho_1 < \exp 16 \cdot 5$ and $D < x_1^4 < (\rho_1/2)^4 < \exp 64$. Thus the theorem.

\[ \square \]

3. Proof of Theorem 2

Lemma 7 [6, Theorems 1 and 2]. Let $D'$ be a nonsquare integer, and let $k$ be an integer with g.c.d. $(k, D') = 1$. If $D' > 0$, $|k| > 1$ and $2 \nmid k$, then every integer solution $(X, Y, Z)$ of the equation

(19) \hspace{1cm} X^2 - D'Y^2 = k^2, \quad \text{g.c.d.} (X, Y) = 1, \quad Z > 0
can be expressed as
\[ Z = Z^r, \quad X + Y\sqrt{D'} = (X_1 \pm Y_1\sqrt{D'})^r(\nu + w\sqrt{D'}), \]
where \( r \) is a positive integer, \((\nu, w)\) is an integer solution of the equation
\[ \nu^2 - D'w^2 = 1, \]
\((X_1, Y_1, Z_1)\) is a positive integer solution of (19) which satisfies
\[ 1 < \left| \frac{X_1 + Y_1\sqrt{D'}}{X_1 - Y_1\sqrt{D'}} \right| < (\nu_1 + w_1\sqrt{D'})^2 \]
and
\[ h(4D') \equiv 0 \pmod{Z_1}, \]
where \( \nu_1 + w_1\sqrt{D'} \) is the fundamental solution of (20), \( h(4D') \) is the class number of binary quadric primitive forms with discriminant \( 4D' \).

Lemma 8 [2, Theorem 2]. Let \( \alpha_1, \ldots, \alpha_n \) be algebraic numbers of the field \( \mathbb{K} = \mathbb{Q}(\alpha_1, \ldots, \alpha_n) \) with heights \( H_1, \ldots, H_n \), respectively, \( A_i = \max(4, H_i) \) \((i = 1, \ldots, n)\), \( A_1 \leq \cdots \leq A_{n-1} \leq A_n \), and let \( d \) denote the degree of \( \mathbb{K} \). If \( \Lambda = b_1 \log \alpha_1 + \cdots + b_n \log \alpha_n \neq 0 \) for some integers \( b_1, \ldots, b_n \), then
\[ |\Lambda| > \exp\left( -\frac{1}{16nd} \cdot 2^{10na} \cdot \log B \cdot \left( \prod_{i=1}^{n} \log A_i \right) \left( \log \prod_{j=1}^{n-1} \log A_j \right) \right), \]
where \( B = \max(4, |b_1|, \ldots, |b_n|) \).

Lemma 9 [1]. Let \( n \) be an integer with \( n \geq 3 \), and let \( f(x) \in \mathbb{Z}[x] \) with degree \( m \) and has at least two simple zeros. Then every integer solution \((x, y)\) of
\[ f(x) = y^n \]
satisfies
\[ \max(|x|, |y|) < \exp\exp((5n)^{10}m^{10m^3}H^{m^2}), \]
where \( H \) is the height of \( f(x) \).

Proof of Theorem 2. If \( m \) in (3) satisfies \( 2| m \), then
\[ x^p = 2z^2 - 1, \]
where \( z = (\varepsilon_1^{m/2} + \varepsilon_1^{m/2})/2 \) is an integer with \( z > 1 \). Then \((1, z, p)\) is an integer solution of the equation
\[ X^2 - 2Y^2 = (-x)^z, \quad \gcd(X, Y) = 1, \quad z > 0. \]
Since \( 3 + 2\sqrt{2} \) is the fundamental solution of the equation
\[ \nu^2 - 2w^2 = 1 \]
and \( h(8) = 1 \). By Lemma 7, we have
\[ 1 + z\sqrt{2} = (X_1 \pm Y_1\sqrt{2})^p(\nu + w\sqrt{2}), \]
where \((u, w)\) is an integer solution of (22), \(X_1, Y_1\) are positive integers and satisfy

\[(24)\]
\[X_1^2 - 2Y_1^2 = -x, \quad \text{g.c.d.} (X_1, Y_1) = 1,
\]
\[(25)\]
\[1 < \left| \frac{X_1 + Y_1\sqrt{2}}{X_1 - Y_1\sqrt{2}} \right| < (3 + 2\sqrt{2})^2.
\]

Let \(e = X_1 + Y_1\sqrt{2}, \quad \bar{e} = X_1 - Y_1\sqrt{2}, \quad \rho = 3 + 2\sqrt{2}, \quad \bar{\rho} = 3 - 2\sqrt{2}\). From (23), (24), and (25), we obtain

\[1 + z\sqrt{2} = \begin{cases} e^p\bar{\rho}^s, \\ -e^p\bar{\rho}^s, \end{cases} \quad 1 - z\sqrt{2} = \begin{cases} \bar{e}^p\rho^s, \\ -\bar{e}^p\rho^s, \end{cases}
\]
where \(s\) is an integer with \(0 \leq s \leq p\). Hence

\[e^p\bar{\rho}^s + \bar{e}^p\rho^s = \pm 2
\]
and

\[(26)\]
\[|p \log \frac{e}{\bar{e}} - 2s \log \rho| = \frac{\sqrt{2}}{z} \sum_{l=0}^{\infty} \frac{(2y^2)^{-l}}{2l + 1} < \frac{2\sqrt{2}}{z}.
\]

Since \(\rho^2 - 6\rho + 1 = 0, x(-e/\bar{e})^2 + 2(X_1^2 + 2Y_1^2)(-e - |\bar{e}|) + x = 0\), and from (25) that \(2(X_1^2 + 2Y_1^2) < 2\rho^2x\). Hence the heights \(H_1, H_2\) of \(\rho, -e/\bar{e}\) satisfy \(H_1 = 6, H_2 < 2\rho^2x\). Since the degree \(d\) of \(Q(\rho, -e - \bar{e}) = Q(\sqrt{2})\) is 2, by Lemma 8, we have

\[\left| p \log \frac{e}{\bar{e}} - 2s \log \rho \right| > \exp(-2^{2400}(\log 2p)(\log 2\rho^2x)(\log 6)(\log \log 6))
\]
\[> \exp(-2^{2400}(\log 2p)(\log 2\rho^2x)).
\]

On combining this with (26) we get

\[\log 4 + 2^{2400}(\log 2p)(\log 2 + \log \rho + \log x) > \frac{1}{2} \log 2 + \log z > \frac{p}{2} \log x,
\]
whence we conclude that

\[(27)\]
\[p < 2^{2415}
\]
since \(x > 1\). Further, by Lemma 9, from (21) we get

\[(28)\]
\[z = \max(x, z) < \exp \exp(2^{84}(5p)^{10}).
\]

Since \(z = (e_1^{m/2} + \bar{e}_1^{m/2})/2 > \sqrt{D}\), substitute (27) into (28) we get \(D < \exp \exp \exp \exp 10\). The theorem is proved. \(\square\)

**Acknowledgment**

The author would like to thank the referee for giving a valuable suggestion to improve Theorem 1.
References


Research Department, Changsha Railway Institute, Changsha, Hunan, China