C O L L O Q U I U M   M A T H E M A T I C U M

VOL. LXVIII 1995 FASC. 2

THE SOLVABILITY OF THE DIOPHANTINE EQUATION $D_1x^2 - D_2y^4 = 1$

BY

MAOHUA LE (ZHANJIANG)

1. Introduction. Let $\mathbb{Z}$, $\mathbb{N}$ denote the sets of integers and positive integers respectively. Let $D_1, D_2 \in \mathbb{N}$ such that $\gcd(D_1, D_2) = 1$ and D_1D_2 is not a square. Many papers concerning the equation

$$(1) \qquad D_1x^2 - D_2y^4 = 1, \quad x, y \in \mathbb{N},$$

were written by Cohn, Ljunggren, Maĭrullin, Mordell and Obláth. In this paper we deal with the solvability of (1). Clearly, if (x, y) is a solution of (1), then (x, y^2) is a solution of the equation

$$(2) \qquad D_1u^2 - D_2v^2 = 1, \quad u, v \in \mathbb{Z},$$

with $x > 0$ and $y^2 > 0$. Since D_1D_2 is not a square, (2) has a unique solution (u_1, v_1) such that $u_1 > 0$, $v_1 > 0$ and $u_1\sqrt{D_1} + v_1\sqrt{D_2} \le u\sqrt{D_1} + v\sqrt{D_2}$, where (u, v) runs over all solutions of (2) with $u > 0$ and $v > 0$. The solution (u_1, v_1) is called the *least solution* of (2). In this paper, using the Ko–Terjanian–Rotkiewicz method (cf. [3]), we prove the following result:

THEOREM. *If* $\min(D_1, D_2) > 1$, *then* (1) *has solutions* (x, y) *if and only if the least solution* (u_1, v_1) *of* (2) *satisfies*

$$(3) \qquad v_1 = dk^2, \quad d, k \in \mathbb{N}, \ d \text{ is square free},$$

and $(\varepsilon_1^d - \overline{\varepsilon}_1^d)/(2\sqrt{D_2})$ *is a square, where*

$$(4) \qquad \varepsilon_1 = u_1\sqrt{D_1} + v_1\sqrt{D_2}, \quad \overline{\varepsilon}_1 = u_1\sqrt{D_1} - v_1\sqrt{D_2}.$$

2. Lemmas

LEMMA 1 ([2]). *For* $\min(D_1, D_2) > 1$, *if* (2) *has solutions* (u, v), *then all solutions* (u, v) *of* (2) *with* $u > 0$ *and* $v > 0$ *are given by*

$$u\sqrt{D_1} + v\sqrt{D_2} = (u_1\sqrt{D_1} + v_1\sqrt{D_2})^t,$$

where $t \in \mathbb{N}$ *with* $2 \nmid t$, *and* (u_1, v_1) *is the least solution of* (2).

1991 *Mathematics Subject Classification*: 11D25, 11A15.
Supported by the National Natural Science Foundation of China.

LEMMA 2 ([1, p. 117]). *For any $n \in \mathbb{N}$ and any complex numbers α, β,*

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

LEMMA 3. *For $\min(D_1, D_2) > 1$, let (u, v) be a solution of (2) with $u > 0$, $v > 0$, and let*

$$\varepsilon = u\sqrt{D_1} + v\sqrt{D_2}, \qquad \overline{\varepsilon} = u\sqrt{D_1} - v\sqrt{D_2}.$$

Further, for any $m \in \mathbb{Z}$ with $2 \nmid m$, let

$$F(m) = \frac{\varepsilon^m - \overline{\varepsilon}^m}{\varepsilon - \overline{\varepsilon}}. \tag{5}$$

Then the $F(m) \in \mathbb{Z}$ satisfy:

(i) *$F(m) = -F(-m)$.*
(ii) *If $m > 0$, then $F(m) \in \mathbb{N}$ satisfies $F(m) \equiv m \pmod{4D_2v^2}$.*
(iii) *For any $m' \in \mathbb{Z}$ with $2 \nmid m'$, $F(m) \equiv F(m - 2m') \pmod{F(m')}$.*

Proof. Since $\varepsilon\overline{\varepsilon} = 1$, we have $F(m) = -F(-m)$. For $m > 0$, by Lemma 2, we get

$$\begin{aligned} F(m) = \frac{\varepsilon^m + (-\overline{\varepsilon})^m}{\varepsilon + (-\overline{\varepsilon})} &= \sum_{i=0}^{(m-1)/2} \frac{m}{i} \binom{m-i-1}{i-1} (\varepsilon - \overline{\varepsilon})^{m-2i-1} (\varepsilon\overline{\varepsilon})^i \\ &= \sum_{i=0}^{(m-1)/2} \frac{m}{i} \binom{m-i-1}{i-1} (4D_2v^2)^{(m-1)/2-i} \\ &\equiv m \pmod{4D_2v^2}. \end{aligned} \tag{6}$$

This implies (ii).

For any $m, m' \in \mathbb{Z}$ with $2 \nmid mm'$, by Lemma 2, we have

$$\begin{aligned} \varepsilon^{m-m'} + \overline{\varepsilon}^{m-m'} &= \varepsilon^{|m-m'|} + \overline{\varepsilon}^{|m-m'|} \\ &= \sum_{j=0}^{|m-m'|/2} (-1)^j \frac{|m-m'|}{j} \binom{|m-m'|-j-1}{j-1} \\ &\quad \times (4D_1u^2)^{|m-m'|/2-j} \in \mathbb{Z}. \end{aligned}$$

Hence, from

$$\frac{\varepsilon^m - \overline{\varepsilon}^m}{\varepsilon - \overline{\varepsilon}} = (\varepsilon\overline{\varepsilon})^{m'} \left(\frac{\varepsilon^{m-2m'} - \overline{\varepsilon}^{m-2m'}}{\varepsilon - \overline{\varepsilon}} \right) + (\varepsilon^{m-m'} + \overline{\varepsilon}^{m-m'}) \left(\frac{\varepsilon^{m'} - \overline{\varepsilon}^{m'}}{\varepsilon - \overline{\varepsilon}} \right)$$

we see that (iii) is true. The lemma is proved.

LEMMA 4. *Let* $m, m_1 \in \mathbb{N}$ *with* $m > m_1 > 1$ *and* $\gcd(m, m_1) = 1$. *Then there exist* $m_2, \ldots, m_s, a_1, \ldots, a_{s-1} \in \mathbb{N}$ *such that*

$$m_1 > m_2 > \ldots > m_s = 1, \quad 2 \nmid m_2 \ldots m_s, \tag{7}$$

$$m = 2a_1 m_1 + \delta_1 m_2, \quad m_{j-1} = 2a_j m_j + \delta_j m_{j+1}, \quad j = 2, \ldots, s-1, \tag{8}$$

where $\delta_i \in \{-1, 1\}$ *for* $i = 1, \ldots, s-1$.

Proof. Use the Euclidean algorithm.

LEMMA 5. *Let* $m, m_1 \in \mathbb{N}$ *satisfy* $m > m_1 > 1$ *and* $\gcd(m, m_1) = 1$, *and let* $m_2, \ldots, m_s, \delta_1, \ldots, \delta_{s-1}$ *be defined as in Lemma* 4. *Then*

$$\left(\frac{m}{m_1}\right) = (-1)^{\Sigma_{i=1}^{s-1} \frac{\delta_i - 1}{2} \cdot \frac{m_i - 1}{2} + \Sigma_{j=1}^{s-2} \frac{m_j - 1}{2} \cdot \frac{m_{j+1} - 1}{2}},$$

where (m/m_1) *is the Jacobi symbol.*

Proof. This is clear from the basic properties of the Jacobi symbol.

LEMMA 6. *Let* $m \in \mathbb{N}$ *satisfy* $m > 1$, $m \equiv 1 \pmod 4$ *and suppose* m *is not a square. Then there exists* $m_1 \in \mathbb{N}$ *such that* $m > m_1 > 1$, $2 \nmid m_1$ *and* $(m/m_1) = -1$.

Proof. By assumption, $m = p_1 \ldots p_r m'^2$, where $p_1, \ldots, p_r$ are distinct odd primes and $m' \in \mathbb{N}$ with $2 \nmid m'$. Then there exists a non-residue a modulo p_1. Further, by the Chinese remainder theorem, there exists a $b \in \mathbb{N}$ such that

$$b \equiv a \pmod{p_1}, \quad b \equiv 1 \pmod{p_j}, \quad j = 2, \ldots, r. \tag{9}$$

Let

$$c = \begin{cases} b & \text{if } \gcd(b, m') = 1, \\ b + p_1 \ldots p_r & \text{if } \gcd(b, m') > 1. \end{cases} \tag{10}$$

Since $\gcd(b, p_1 \ldots p_r) = 1$ by (9), we see from (10) that $c \in \mathbb{Z}$ with $\gcd(c, m) = 1$. Hence, by (9) and (10), we get

$$\begin{aligned} \left(\frac{c}{m}\right) &= \left(\frac{c}{p_1}\right) \ldots \left(\frac{c}{p_r}\right)\left(\frac{c}{m'^2}\right) = \left(\frac{c}{p_1}\right) \ldots \left(\frac{c}{p_r}\right) \\ &= \left(\frac{b}{p_1}\right) \ldots \left(\frac{b}{p_r}\right) = \left(\frac{a}{p_1}\right) = -1. \end{aligned} \tag{11}$$

Let $c_0, m_1 \in \mathbb{Z}$ satisfy $c_0 \equiv c \pmod m$, $0 \le c_0 < m$ and

$$m_1 = \begin{cases} c_0 & \text{if } 2 \nmid c_0, \\ m - c_0 & \text{if } 2 \mid c_0. \end{cases}$$

Notice that $m \equiv 1 \pmod 4$ and $2 \nmid m_1$. We see from (11) that $(m/m_1) = -1$. The lemma is proved.

Lemma 7. *The equation*

$$F(m) = z^2, \quad m, z \in \mathbb{N},\ m > 1,\ 2 \nmid m \text{ and } m \text{ is not a square}, \tag{12}$$

has no solution (m, z).

This is a special case ($M = 1$, $L = 4u^2 D_1$) of Theorem 3 of [3].

3. Proof of Theorem. The sufficiency being clear, it suffices to prove the necessity. Assume that (1) has solutions (x, y). Then (1) has a unique solution (x_1, y_1) such that

$$x_1\sqrt{D_1} + y_1^2\sqrt{D_2} \le x\sqrt{D_1} + y^2\sqrt{D_2}, \tag{13}$$

where (x, y) runs over all solutions of (1). Notice that (x_1, y_1^2) is a solution of (2) with $x_1, y_1^2 \in \mathbb{N}$. Let (u_1, v_1) be the least solution of (2). By Lemma 1, we have

$$x_1\sqrt{D_1} + y_1^2\sqrt{D_2} = (u_1\sqrt{D_1} + v_1\sqrt{D_2})^t, \tag{14}$$

where $t \in \mathbb{N}$ with $2 \nmid t$.

If $t = 1$, then (14) shows that $v_1 = y_1^2$ and the theorem holds. Let ε_1, $\overline{\varepsilon}_1$ be defined as in (4), and let

$$F_1(m) = \frac{\varepsilon_1^m - \overline{\varepsilon}_1^m}{\varepsilon_1 - \overline{\varepsilon}_1}$$

for any $m \in \mathbb{Z}$ with $2 \nmid m$. If $t > 1$, then

$$y_1^2 = \frac{\varepsilon_1^t - \overline{\varepsilon}_1^t}{2\sqrt{D_2}} = v_1 F_1(t), \tag{15}$$

by (14). We deduce from (15) that

$$v_1 = c_1 y_{11}^2 \tag{16}$$

and

$$F_1(t) = c_1 y_{12}^2, \tag{17}$$

where $c_1, y_{11}, y_{12} \in \mathbb{N}$ satisfy $c_1 y_{11} y_{12} = y_1$. By Lemma 3(ii), we have $F(t) \equiv t \pmod{v_1}$, hence, by (16) and (17),

$$t \equiv 0 \pmod{c_1}. \tag{18}$$

We now suppose that t has a divisor p^2, where p is an odd prime. Let

$$\begin{aligned} u_2\sqrt{D_1} + v_2\sqrt{D_2} &= (u_1\sqrt{D_1} + v_1\sqrt{D_2})^{t/p}, \\ u_3\sqrt{D_1} + v_3\sqrt{D_2} &= (u_1\sqrt{D_1} + v_1\sqrt{D_2})^{t/p^2}. \end{aligned} \tag{19}$$

By Lemma 1, (u_2, v_2) and (u_3, v_3) are solutions of (2) with $u_2, v_2, u_3, v_3 \in \mathbb{N}$. Further, let

$$\begin{aligned} \varepsilon_2 &= u_2\sqrt{D_1} + v_2\sqrt{D_2}, \quad \overline{\varepsilon}_2 = u_2\sqrt{D_1} - v_2\sqrt{D_2}, \\ \varepsilon_3 &= u_3\sqrt{D_1} + v_3\sqrt{D_2}, \quad \overline{\varepsilon}_3 = u_3\sqrt{D_1} - v_3\sqrt{D_2}, \end{aligned} \tag{20}$$

and let

$$F_2(m) = \frac{\varepsilon_2^m - \overline{\varepsilon}_2^m}{\varepsilon_2 - \overline{\varepsilon}_2}, \qquad F_3(m) = \frac{\varepsilon_3^m - \overline{\varepsilon}_3^m}{\varepsilon_3 - \overline{\varepsilon}_3}, \tag{21}$$

for any $m \in \mathbb{Z}$ with $2 \nmid m$. Then, by (14), we have

$$y_1^2 = \frac{\varepsilon_2^p - \overline{\varepsilon}_2^p}{2\sqrt{D_2}} = v_2 F_2(p).$$

This implies that

$$v_2 = c_2 y_{11}'^2, \qquad F_2(p) = c_2 y_{12}'^2, \tag{22}$$

where $c_2, y_{11}', y_{12}' \in \mathbb{N}$ satisfy $c_2 y_{11}' y_{12}' = y_1$. By Lemma 3(ii), $F_2(p) \equiv p \pmod{v_2}$, hence, by (22), $p \equiv 0 \pmod{c_2}$. This implies that either $c_2 = 1$ or $c_2 = p$. From (22), if $c_2 = 1$, then $F_2(p)$ is a square, which is impossible by Lemma 7. Therefore, $c_2 = p$ and

$$v_2 = p y_{11}'^2, \qquad F_2(p) = p y_{12}'^2, \tag{23}$$

by (22). On the other hand, we see from (19)–(21) that

$$v_2 = v_3 F_3(p). \tag{24}$$

The combination of (23) and (24) yields

$$v_3 = \begin{cases} c_3 y_{111}^2, \\ c_3 p y_{112}^2, \end{cases} \qquad F_3(p) = \begin{cases} c_3 p y_{112}^2, \\ c_3 y_{111}^2, \end{cases} \tag{25}$$

where $c_3, y_{111}, y_{112} \in \mathbb{N}$ satisfy $c_3 y_{111} y_{112} = y_{11}'$. Notice that $F_3(p)$ is never a square by Lemma 7. By much the same argument as above, we can find from (25) that $c_3 = 1$ or p, and v_3 is a square. Since (u_3, v_3) is a solution of (2), it follows that $(u_3, \sqrt{v_3})$ is a solution of (1) satisfying $u_3\sqrt{D_1} + v_3\sqrt{D_2} < x_1\sqrt{D_1} + y_1^2\sqrt{D_2}$ by (19), which contradicts our assumption (13). Thus, t is square free and so is c_1 by (18).

If $t \neq c_1$, then t has an odd prime divisor q with $q \nmid c_1$ by (18). Let

$$u_4\sqrt{D_1} + v_4\sqrt{D_2} = (u_1\sqrt{D_1} + v_1\sqrt{D_2})^{t/q}, \tag{26}$$

$$\varepsilon_4 = u_4\sqrt{D_1} + v_4\sqrt{D_2}, \qquad \overline{\varepsilon}_4 = u_4\sqrt{D_1} - v_4\sqrt{D_2}, \tag{27}$$

and let

$$F_4(m) = \frac{\varepsilon_4^m - \overline{\varepsilon}_4^m}{\varepsilon_4 - \overline{\varepsilon}_4} \tag{28}$$

for any $m \in \mathbb{Z}$ with $2 \nmid m$. Then, by (14) and (26)–(28), we have $y_1^2 = v_4 F_4(q)$, whence

$$v_4 = c_4 y_{13}^2, \qquad F_4(q) = c_4 y_{14}^2, \tag{29}$$

where $c_4, y_{13}, y_{14} \in \mathbb{N}$ satisfy $c_4 y_{13} y_{14} = y_1$. Using the same method, by (26) and (29), we can prove that $c_4 = q$ and

$$v_4 = q y_{13}^2 = \frac{\varepsilon_1^{t/q} - \overline{\varepsilon}_1^{t/q}}{2\sqrt{D_2}} = v_1 F_1(t/q). \tag{30}$$

Substituting (16) into (30) gives

$$F_1\left(\frac{t}{q}\right) = \frac{q y_{13}^2}{c_1 y_{11}^2}. \tag{31}$$

Notice that $F_1(t/q) \in \mathbb{N}$ and $q \nmid c_1$. We see from (31) that $q \mid y_{11}$, $q \mid y_{13}$, $q \mid F_1(t/q)$ and $q \mid v_1$ by (16), a contradiction. Thus, we deduce that $t = c_1$ and the necessity is proved by (14) and (16), since t is square free. The proof is complete.

Remark. By much the same argument as in the proof of the Theorem, we can prove a similar result for the case $\min(D_1, D_2) = 1$.

REFERENCES

[1] R. Lidl and H. Niederreiter, *Finite Fields*, Addison-Wesley, Reading, Mass., 1983.
[2] K. Petr, *Sur l'équation de Pell*, Časopis Pěst. Mat. Fys. 56 (1927), 57–66.
[3] A. Rotkiewicz, *Applications of Jacobi's symbol to Lehmer's numbers*, Acta Arith. 42 (1983), 163–187.

DEPARTMENT OF MATHEMATICS
ZHANJIANG TEACHER'S COLLEGE
P.O. BOX 524048
ZHANJIANG, GUANGDONG
P.R. CHINA

Reçu par la Rédaction le 26.4.1993