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

VOL. 71 | 1996 | NO. 1

A NOTE ON THE DIOPHANTINE EQUATION $(x^2-1)(y^2-1)=(z^2-1)^2$

BY

HUAMING WU AND MAOHUA LE (ZHANJIANG)

1. Introduction. Let $\mathbb{Z}$, $\mathbb{N}$ be the sets of integers and positive integers respectively. In this note we deal with the solutions (x,y,z) of the equation

(1) $$(x^2-1)(y^2-1)=(z^2-1)^2, \quad x,y,z\in\mathbb{N},\ x>z>y>1.$$

Schinzel and Sierpiński [3] found all solutions of (1) with $x-y=2z$. Grelak [2] proved that if (x,y,z) is a solution of (1) and satisfies $2\mid x$ and $2\mid y$, then $\operatorname{pot}_2 x=\operatorname{pot}_2 y$. Wang [4] and Cao [1] proved that (1) has no solutions (x,y,z) satisfying $x-y=z$ or $x-y=kz$ with $2<k\le 30$ respectively. In this note, using some properties of Pell's equation, we prove the following general result:

THEOREM. *Equation* (1) *has no solutions* (x,y,z) *satisfying* $2\mid x$, $2\mid y$ *and* $x-y=kz$, *where* $k\in\mathbb{N}$ *with* $k>2$.

2. Preliminaries. Let $D\in\mathbb{N}$ be nonsquare, and let (u,v) be a positive integer solution of Pell's equation

(2) $$u^2-Dv^2=1, \quad u,v\in\mathbb{Z}.$$

For any $t\in\mathbb{N}$, let $u_t,v_t\in\mathbb{N}$ satisfy

(3) $$u_t+v_t\sqrt{D}=(u+v\sqrt{D})^t.$$

LEMMA 1. *If* $2\mid u_t$, *then* $2\nmid t$.

Proof. Since $2\mid Duv$ by (2), we see from (3) that if $2\mid t$, then $2\mid v_t$ and $2\nmid u_t$. The lemma is proved.

LEMMA 2. *If* $\gcd(v_r,v_s)=1$, *then* $\gcd(r,s)=1$.

Proof. Let $d=\gcd(r,s)$. By (3), we have $v_d\mid v_r$ and $v_d\mid v_s$. Since $v_d>1$ if $d>1$, we get $d=1$ if $\gcd(v_r,v_s)=1$. The lemma is proved.

1991 *Mathematics Subject Classification*: 11D25, 11D09.

Supported by the National Natural Science Foundation of China and the Guandong Provincial Natural Science Foundation.

LEMMA 3. *If* $r > s$, $2 \nmid r$, $2 \nmid s$, $r \equiv s \pmod 4$ *and* $\gcd(r,s) = 1$, *then* $\gcd(u_{(r+s)/2}, v_{(r-s)/2}) = u_1$.

Proof. Let $\varepsilon = u + v\sqrt{D}$ and $\overline{\varepsilon} = u - v\sqrt{D}$. By (3), we get

$$u_t = \frac{\varepsilon^t + \overline{\varepsilon}^t}{2}, \quad v_t = \frac{\varepsilon^t - \overline{\varepsilon}^t}{2\sqrt{D}}, \quad t \in \mathbb{N}.$$

Let $d = \gcd(u_{(r+s)/2}, v_{(r-s)/2})$. Then we have

$$(4) \qquad \varepsilon^{(r+s)/2} \equiv -\overline{\varepsilon}^{(r+s)/2} \pmod{2d}, \qquad \varepsilon^{(r-s)/2} \equiv \overline{\varepsilon}^{(r-s)/2} \pmod{2d}.$$

Since $\varepsilon\overline{\varepsilon} = 1$, we deduce from (4) that

$$(5) \qquad u_r \equiv 0 \pmod d, \qquad u_s \equiv 0 \pmod d.$$

Since $\gcd(r,s) = 1$, there exist $\alpha, \beta \in \mathbb{Z}$ such that $\alpha r - \beta s = 1$. Hence, by (5), we get

$$(6) \qquad \varepsilon^{\alpha r - \beta s} - (-1)^{\alpha+\beta}\overline{\varepsilon}^{\alpha r - \beta s} = \varepsilon - (-1)^{\alpha+\beta}\overline{\varepsilon} \pmod{2d}.$$

Notice that $2 \nmid r$ and $2 \nmid s$. We have $\alpha + \beta \equiv 1 \pmod 2$ and

$$(7) \qquad u_1 \equiv 0 \pmod d,$$

by (6). On the other hand, we see from (3) that $u_1 \mid u_{(r+s)/2}$ and $u_1 \mid v_{(r-s)/2}$ if $r \equiv s \pmod 4$. This implies that $d \equiv 0 \pmod{u_1}$. On combining this with (7) we get $d = u_1$. The lemma is proved.

3. Proof of Theorem. Let (x,y,z) be a solution of (1) which satisfies $2 \mid x$, $2 \mid y$ and $x - y = kz$ with $k \in \mathbb{N}$. Then

$$(8) \qquad x^2 - 1 = Da^2, \qquad y^2 - 1 = Db^2,$$

where $a, b, D \in \mathbb{N}$ satisfy

$$(9) \qquad z^2 - 1 = Dab, \qquad \gcd(a,b) = 1.$$

By (8), D is not a square, and $(u,v) = (x,a)$ and (y,b) are positive integer solutions of Pell's equation (2).

Let $\varepsilon = u_1 + v_1\sqrt{D}$ be the fundamental solution of (2), and let $\overline{\varepsilon} = u_1 - v_1\sqrt{D}$. Since $x > y$, we see from (8) that

$$(10) \qquad x + a\sqrt{D} = \varepsilon^r, \quad x - a\sqrt{D} = \overline{\varepsilon}^r,$$

$$(11) \qquad y + b\sqrt{D} = \varepsilon^s, \quad y - b\sqrt{D} = \overline{\varepsilon}^s,$$

where $r, s \in \mathbb{N}$ with $r > s$. Notice that $2 \mid x$, $2 \mid y$ and $\gcd(a,b) = 1$. By Lemmas 1 and 2, we find that $2 \nmid r$, $2 \nmid s$ and $\gcd(r,s) = 1$ respectively.

For any $t \in \mathbb{N}$, let $\varepsilon^t = u_t + v_t\sqrt{D}$. Then $u_t, v_t \in \mathbb{N}$ satisfy $\overline{\varepsilon}^t = u_t - v_t\sqrt{D}$ and $u_t^2 - Dv_t^2 = 1$. Let $m = (r+s)/2$ and $n = (r-s)/2$. From (10) and (11), we get

$$(12) \qquad x = u_r = u_m u_n + D v_m v_n, \qquad y = u_s = u_m u_n - D v_m v_n,$$

$$Dab = Dv_r v_s = \tfrac{1}{2}(u_{r+s} - u_{r-s}) = u_m^2 - u_n^2 = Dv_m^2 - Dv_n^2. \tag{13}$$

By (9) and (13), we obtain

$$z^2 = Dv_m^2 - Dv_n^2 + 1. \tag{14}$$

On the other hand, since $x - y = kz$, we deduce from (12) and (14) that

$$2Dv_m v_n = kz. \tag{15}$$

Hence, by (14) and (15),

$$k^2(Dv_m^2 - Dv_n^2 + 1) = 4D^2 v_m^2 v_n^2. \tag{16}$$

Since $\gcd(D, Dv_m^2 - Dv_n^2 + 1) = 1$, we see from (16) that $k = Dk_1$, and

$$k_1^2(Dv_m^2 - Dv_n^2 + 1) = 4v_m^2 v_n^2, \qquad k_1 \in \mathbb{N}. \tag{17}$$

Since $2 \mid x$ and $2 \nmid r$, we see from (10) that $2 \mid u_1$. Let $2^\alpha \parallel u_1$. If $r \not\equiv s \pmod 4$, then $2 \mid m$, $2 \nmid n$ and

$$2 \parallel Dv_m^2 - Dv_n^2 + 1 = Dv_m^2 - u_n^2 + 2.$$

This implies that (17) is impossible in this case. So we have $r \equiv s \pmod 4$. Then $2 \nmid m$, $2 \mid n$ and

$$2^{2\alpha} \parallel Dv_m^2 - Dv_n^2 + 1 = u_m^2 - Dv_n^2. \tag{18}$$

Since $2 \mid n$ and $2^{\alpha+1} \mid v_n$, we see from (17) and (18) that $k_1 = 2k_2$ and

$$k_2^2(Dv_m^2 - Dv_n^2 + 1) = v_m^2 v_n^2, \qquad k_2 \in \mathbb{N}. \tag{19}$$

Recall that $2 \nmid r$, $2 \nmid s$, $\gcd(r, s) = 1$ and $2 \mid n$. By Lemma 3, we have $\gcd(u_m, v_n) = u_1$. Since $Dv_m^2 - Dv_n^2 + 1 = u_m^2 - Dv_n^2$, we see from (19) that $k_2 = k_3(v_n/u_1)$ and

$$k_3^2(Dv_m^2 - Dv_n^2 + 1) = v_m^2 u_1^2, \qquad k_3 \in \mathbb{N}. \tag{20}$$

Further, by (20), we get

$$k_3 = v_{m1}k_4, \quad Dv_m^2 - Dv_n^2 + 1 = v_{m2}^2 u_1^2, \quad k_4 \in \mathbb{N}, \tag{21}$$

where $v_{m1}, v_{m2} \in \mathbb{N}$ with $v_{m1}v_{m2} = v_m$. Since $v_{m2} \mid v_m$, we see from (21) that $v_{m2}^2 \mid Dv_n^2 - 1$. So we have

$$Dv_n^2 - 1 = u_n^2 - 2 = lv_{m2}^2, \qquad l \in \mathbb{N}. \tag{22}$$

Since $2 \mid n$ and $2 \nmid u_n^2$, by (22), we get $l \equiv lv_{m2}^2 = u_n^2 - 2 \equiv 7 \pmod 8$. It implies that $l \geq 7$. Hence, we obtain

$$v_{m2}^2 \leq \frac{Dv_n^2 - 1}{7}. \tag{23}$$

From (21) and (23), we get

$$Dv_m^2 = (Dv_n^2 - 1) + v_{m2}^2 u_1^2 \leq (Dv_n^2 - 1)\left(1 + \frac{u_1^2}{7}\right) < Dv_n^2\left(1 + \frac{u_1^2}{7}\right). \tag{24}$$

Since $\varepsilon\overline{\varepsilon} = 1$, by (24), we deduce that

$$u_1 + 1 < u_1 + v_1\sqrt{D} = \varepsilon \le \varepsilon^s = \varepsilon^{m-n} < \varepsilon^{m-n} - \frac{\varepsilon^{m-2n} - \varepsilon^{-m}}{\varepsilon^n - \overline{\varepsilon}^n}$$
$$= \frac{\varepsilon^m - \overline{\varepsilon}^m}{\varepsilon^n - \overline{\varepsilon}^n} = \frac{v_m}{v_n} < \left(1 + \frac{u_1^2}{7}\right)^{1/2} < u_1 + 1,$$

a contradiction. The theorem is proved.

REFERENCES

[1] Z.-F. Cao, *A generalization of the Schinzel–Sierpiński system of equations*, J. Harbin Inst. Tech. 23 (5) (1991), 9–14 (in Chinese).

[2] A. Grelak, *On the diophantine equation* $(x^2-1)(y^2-1) = (z^2-1)^2$, Discuss. Math. 5 (1982), 41–43.

[3] A. Schinzel and W. Sierpiński, *Sur l'équation diophantienne* $(x^2-1)(y^2-1) = [((y-x)/2)^2-1]^2$, Elem. Math. 18 (1963), 132–133.

[4] Y.-B. Wang, *On the diophantine equation* $(x^2-1)(y^2-1) = (z^2-1)^2$, Heilongjiang Daxue Ziran Kexue Xuebao 1989, (4), 84–85 (in Chinese).

Department of Mathematics
Zhanjiang Teachers' College
P.O. Box 524048
Zhanjiang, Guangdong
P.R. China

Received 6 December 1995