ON SOME EQUATIONS RELATED TO MA'S CONJECTURE

Jiagui Luo
College of Mathematics and Information Science, Zhaoqing University, Zhaoqing, P. R. China
Luojg62@yahoo.com.cn

Alain Togbé
Mathematics Department, Purdue University North Central, Westville Indiana
atogbe@pnc.edu

Pingzhi Yuan
School of Mathematics, South China Normal University, Guangzhou, P. R. China
mcsypz@mail.sysu.edu.cn

Received: 9/15/10, Revised: 12/1/10, Accepted: 2/8/11, Published: 5/6/11

Abstract

In 1992, Ma made a conjecture related to Pell equations. In this paper, we use Störmer's Theorem and related results on Pell equations to prove some particular cases of Ma's conjecture.

1. Introduction

There are many papers studying the positive integer solutions and the minimal positive solutions of the diophantine equations

$$kx^2 - ly^2 = C,\ C = 1,\ 2,\ 4, \tag{1}$$

and the relations between these solutions. Throughout this paper, we assume that k, l are coprime positive integers and kl is not a square. Suppose that $2 \nmid kl$ when $C = 2$ or 4. A well-known and interesting result is Störmer's Theorem had been obtained. An application of Störmer's Theorem is Ma's conjecture. Let $\mathbb{N}_0$ be the set of all nonnegative integers. In 1992, S. L. Ma [13] presented the following conjecture.

Conjecture 1. Let p an odd prime and $a \geq 0,\ b, t, r \geq 1$. Then

(A) $Y = 2^{2a+2}p^{2t} - 2^{2a+2}p^{t+r} + 1$ is a square if and only if $t = r$, that is, if and only if $Y = 1$.

(B) $Z = 2^{2b+2}p^{2t} - 2^{b+2}p^{t+r} + 1$ is a square if and only if $p = 5, b = 3, t = 1$, and $r = 2$, that is, if and only if $Z = 2401$.

Ma proved that Conjecture 1 implies McFarland's conjecture on Abelian difference sets with multiplier -1. Moreover, Zhenfu Cao [1] and later Le-Xiang [8] obtained a proof of Conjecture 1(A).

The aim of this paper is not only to give an extension of Ma's conjecture but also to obtain another application of Störmer's Theorem. First, we consider the Diophantine equation

$$x^2 = p^{2a}k_1^{2t_1}\cdots k_s^{2t_s}y^2 - p^{a+b}k_1^{t_1+r_1}\cdots k_s^{t_s+r_s}\delta + 1,\ \delta \in \{-2,-4,2,4\}, \qquad (2)$$

where

$$x, y, a, b, k_i, t_i \in \mathbb{N},\ i = 1, 2, \cdots, s,\ r_i \in \mathbb{N}_0,\ i = 1, 2, \cdots, s,\ 2 \nmid y,$$

and p is an odd prime. Using Theorems 8, 11, and 15 we obtain the following result.

Theorem 2. *Let $t_i > r_i$ $(i = 1, 2, \cdots, s)$, $a \geq b$ and $k_1, k_2, \cdots k_s > 1$ be odd.*

(i) *Assume that $\delta = -2$ or $\delta = 2$. Then the only solutions to equation (2) are given by:*

(A) *If $p|y$, then*

$$x = p^{a+b}k_1^{t_1+r_1}\cdots k_s^{t_s+r_s} - \frac{\delta}{2},\ y = p^b k_1^{r_1}\cdots k_s^{r_s}.$$

(B) *If $\delta = 2$ and*

$$p^b = 3^t + 2 = 2\cdot 3^{-2t}k_1^{t_1+r_1}\cdots k_s^{t_s+r_s} - 1,\ 2 \nmid t,$$

then

$$x = \frac{1}{2}(p^b - 1)((p^b - 1)^2 - 3),\ y = 3^{-t}k_1^{r_1}\cdots k_s^{r_s},\ a = b.$$

(C) *If $\delta = -2$ and*

$$p^b = 3^t - 2 = 2\cdot 3^{-2t}k_1^{t_1+r_1}\cdots k_s^{t_s+r_s} + 1,\ 2|t,$$

then

$$x = \frac{1}{2}(p^b + 1)((p^b + 1)^2 - 3),\ y = 3^{-t}k_1^{r_1}\cdots k_s^{r_s},\ a = b.$$

(ii) *Assume that $\delta = -4$ or $\delta = 4$. Then the Diophantine equation (2) has no positive integer solutions.*

Second, we consider the Diophantine equation

$$x^2 = p^{2a}k_1^{2t_1}\cdots k_s^{2t_s}y^2 - p^{a+b}k_1^{t_1+r_1}\cdots k_s^{t_s+r_s}\delta + 4,\ \delta \in \{-4,4\}, \qquad (3)$$

where

$$x, y, a, b, k_i, t_i \in \mathbb{N},\ i = 1, 2, \cdots, s,\ r_i \in \mathbb{N}_0,\ i = 1, 2, \cdots, s,\ 2 \nmid y,$$

and p is an odd prime. Using Theorems 9 and 13, we prove the following result.

Theorem 3. *Let $t_i > r_i$ $(i = 1, 2, \cdots, s)$, $a \geq b$ and $k_1, k_2, \cdots k_s > 1$ be odd. Then except for $(x, y, p, s, r_1, t_1, k_1, a, b, \delta) = (123, 1, 11, 1, 1, 2, 5, 1, 1, 4)$, the only solutions to equation (3) are given by:*

(A) *If $p \mid y$, then*

$$x = p^{a+b} k_1^{t_1+r_1} \cdots k_s^{t_s+r_s} - \frac{\delta}{2},\ y = p^b k_1^{r_1} \cdots k_s^{r_s}.$$

(B) *If $p \nmid y$ and $p^b = k_1^{t_1+r_1} \cdots k_s^{t_s+r_s} - \frac{\delta}{2}$, then*

$$x = p^{2b} - 2,\ y = k_1^{r_1} \cdots k_s^{r_s},\ a = b.$$

Some similar equations were studied by Z. Cao [1], Y. D. Guo [5], Z. Cao and A. Grytczuk [2], and X. Dong and Z. Cao [4]. For more details, one can read these references. We organize this paper as follows. In Section 2, we introduce some lemmas that will be useful for the proofs of the main results. So we recall some properties on Pell equations, Störmer's Theorem, and other results on Pell equations that we will use to prove our two main results. Section 3 is devoted to the proofs of Theorems 2 and 3 that are related to Ma's conjecture, i.e., other applications of Störmer's Theorem.

2. Preliminaries

We recall that the minimal positive solution of Equation (1) is one of the positive integer solutions (x, y) such that $x\sqrt{k} + y\sqrt{l}$ is the smallest. One can easily see that this is equivalent to determining a positive integer solution (x, y) of (1) such that x and y are the smallest. If $k = C = 1$ or $l = C = 1$, then such a solution is also called the *fundamental solution* of (1). If $k = C = 1$ or $k = 1, C = 4$, and $x_1 + y_1\sqrt{l}$ is the fundamental solution of (1), then we have the following result.

Lemma 4. ([15]) *All positive integer solutions of* (1) *are given by*

$$\frac{x + y\sqrt{l}}{\sqrt{C}} = \left(\frac{x_1 + y_1\sqrt{l}}{\sqrt{C}}\right)^n,\ n \in \mathbb{N}.$$

If $k > 1$ or $C = 2$, and $x_1\sqrt{k} + y_1\sqrt{l}$ is the minimal positive solution of (1), then we have the following lemma.

Lemma 5. ([10], [15]) *All positive integer solutions of* (1) *are given by*

$$\frac{x\sqrt{k} + y\sqrt{l}}{\sqrt{C}} = \left[\frac{x_1\sqrt{k} + y_1\sqrt{l}}{\sqrt{C}}\right]^n,\ n \in \mathbb{N},\ 2 \nmid n.$$

Let $R > 0$, Q be nonzero coprime integers such that $R - 4Q > 0$. Let α and β be the two roots of the trinomial $x^2 - \sqrt{R}x + Q$. The Lehmer sequence $\{P_n(R, Q)\}$ and the associated Lehmer sequence $\{Q_n(R, Q)\}$ with parameters R and Q are defined as follows:

$$P_n = P_n(R, Q) = \begin{cases} (\alpha^n - \beta^n)/(\alpha - \beta), & 2 \nmid n, \\ (\alpha^n - \beta^n)/(\alpha^2 - \beta^2), & 2|n, \end{cases}$$

and

$$Q_n = Q_n(R, Q) = \begin{cases} (\alpha^n + \beta^n)/(\alpha + \beta), & 2 \nmid n, \\ \alpha^n + \beta^n, & 2|n. \end{cases}$$

For simplicity, in this paper we denote $(\alpha^{dr} - \beta^{dr})/(\alpha^d - \beta^d)$ and $(\alpha^r - \beta^r)/(\alpha - \beta)$ by $P_{r,d}$ and P_r, respectively.

Lehmer sequences and associated Lehmer sequences have many interesting properties and are used in the study of exponential Diophantine equations. It is not difficult to see that P_n and Q_n are both positive integers for all positive integers n. More details can be seen in [9], [14], [18], [17].

Proposition 6. Let m, n be integers and $d = \gcd(m, n)$. We have

1. If $P_m \neq 1$, then $P_m | P_n$ if and only if $m|n$.
2. If $m \geq 1$, then $Q_m | Q_n$ if and only if n/m is an odd integer.
3. $\gcd(P_m, P_n) = U_d$.
4. $\gcd(Q_m, Q_n) = Q_d$ if m/d and n/d are odd, and 1 otherwise.
5. $\gcd(P_m, Q_n) = Q_d$ if m/d is even, and 1 otherwise.
6. $P_{2m} = 2P_m Q_m$.
7. For any prime p, $ord_p(P_{mp}/P_m) = 1$ or 0 depending on whether $p \mid P_m$ or not.

We also recall the following result.

Lemma 7. ([11]) *Assume that R and Q are odd integers. If $Q_n = ku^2$, $k|n$, then $n = 1, 3, 5$. If $Q_n = 2ku^2$, $k|n$, then $n = 3$.*

Störmer obtained an important property on Pell equations, called Störmer's Theorem and stated it as follows.

Theorem 8. (Störmer's Theorem [3]) *Let D be a positive nonsquare integer. Let (x_1, y_1) be a positive integer solution of the Pell equation*

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

If every prime divisor of y_1 divides D, then $x_1 + y_1\sqrt{D}$ is the fundamental solution.

In 1991, Luo obtained an extension of Störmer's Theorem.

Theorem 9. ([10]) *Let (x, y) be a positive integer solution of the Diophantine equation*

$$kx^2 - ly^2 = 4,\ k > 1. \tag{5}$$

(i) *If every prime divisor of x divides k, then $\varepsilon = x\sqrt{k}+y\sqrt{l}$ is the minimal positive solution of equation* (5) *except for the case $(k, l, x, y) = (5, 1, 5, 11)$.*

(ii) *If every prime divisor of y divides l, then $\varepsilon = x\sqrt{k}+y\sqrt{l}$ is the minimal positive solution of equation* (5).

Remark 10. From the proof of Theorem 9 in [10], [15], [16], one can easily observe that the above theorem is also true if every prime divisor of x divides k or x_1, and if every prime divisor of y divides l or y_1.

H. Mei, L. Mei, Q. Fan, and W. Song showed the following theorem.

Theorem 11. ([12]) *Let D be a positive nonsquare integer. Let (x, y) be a positive integer solution of the Pell equation*

$$x^2 - Dy^2 = 1, \tag{6}$$

with $y = p^n y'$, where p is a prime not dividing D and $n \in \mathbb{N}$. If every prime divisor of y' divides D, then $x + y\sqrt{D} = \varepsilon$ or ε^2 or ε^3, where $\varepsilon = x_1 + y_1\sqrt{D}$ is the fundamental solution of (6).

Remarks 12.

1. If $x + y\sqrt{D} = \varepsilon^3$, then $y = 3^s p^n y_1, s \in \mathbb{N}, s > 1$ except for $(x, y, D) = (26, 15, 3)$.
2. A similar result was obtained by A. Grelak, A. Grytczuk [6]. But the above theorem gives more details on different possible cases useful for the proof of Theorem 2.

Now we prove the following theorem.

Theorem 13. *Let D be a positive nonsquare integer such that the Diophantine equation*

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

is solvable in odd integers x and y. Let (x, y) be a positive integer solution of the Pell equation (7) *with $y = p^n y'$, where p is a prime not dividing D and $n \in \mathbb{N}$. If every prime divisor of y' divides D, then $\frac{x+y\sqrt{D}}{2} = \frac{\varepsilon}{2}$ or $(\frac{\varepsilon}{2})^2$ or $(\frac{\varepsilon}{2})^3$ except for the case $(x, y, D) = (123, 55, 5)$, where $\varepsilon = x_1 + y_1\sqrt{D}$ is the minimal positive solution of* (7).

Proof. It is easy to see that the result is true if $p|y_1$ by Remark 10. We assume that $p \nmid y_1$. By Lemma 4, we know that

$$\frac{x+y\sqrt{D}}{2} = \left(\frac{x_1+y_1\sqrt{D}}{2}\right)^m, \tag{8}$$

for some positive integer m. If $m = 1$, there is nothing to do.

`Case 1.` We assume $2|m$. We write $m = 2m_1$. From equation (8), we get

$$\frac{x+y\sqrt{D}}{2} = \left(\frac{x_{m_1}+y_{m_1}\sqrt{D}}{2}\right)^2. \tag{9}$$

Hence

$$x_{m_1}y_{m_1} = p^n y'.$$

Since $x_{m_1}^2 - Dy_{m_1}^2 = 4$, we have that $(x_{m_1}, y_{m_1}) = 1$ or 2. If $(x_{m_1}, y_{m_1}) = 1$, then $y_{m_1} = y'$. It follows that every prime divisor of y_{m_1} divides D. By Theorem 9, we obtain $m_1 = 1$, whence $m = 2$. If $(x_{m_1}, y_{m_1}) = 2$, then $p = 2$, and we have $x_{m_1} = 2^{n-1}$ and $Q_{m_1} = 2^t$. By Lemma 7 and Proposition 6, we have $m_1 = 3$. This implies that $x_1|2^{n-1} = x_3$, which is impossible since x_1 is an odd greater than 1.

`Case 2.` Now we assume $2 \nmid m$. We write $m = m_1 q^r$, where q is a prime divisor of m, $(m_1, q) = 1$, $r \in \mathbb{N}$. We claim that $p|P_q$. Otherwise, every prime divisor of $y_q = y_1 P_q$ divides D by the assumption. It follows that $q = 1$ by Theorem 9. This leads to a contradiction. By Proposition 6, we know that $(P_{m_1}, P_q) = P_{(m_1,q)} = P_1 = 1$. This implies that every prime divisor of $y_{m_1} = y_1 P_{m_1}$ divides D since $y_{m_1}|y_m = y = p^n y'$. Thus we obtain $m_1 = 1$ by Theorem 9. Therefore, we have $m = q^r$. It is obvious that $q \neq p$ since

$$P_q = \sum_{r=0}^{(q-1)/2} \binom{q}{2r+1} (x_1/2)^{q-2r-1} (Dy_1^2/4)^r. \tag{10}$$

If $r > 1$, then

$$P_{q,q} = \sum_{r=0}^{(q-1)/2} \binom{q}{2r+1} (x_q/2)^{q-2r-1} (Dy_q^2/4)^r. \tag{11}$$

We will prove that $q = 3$, $P_{q,q} = 3^t$, and $3|D$. Since $P_3 = (3x_1^2 + Dy_1^2)/4$, we get $3|P_3$ so $3|y_3$. If $t = 1$, from (11) we have $12 = 3x_3^2 + Dy_3^2 = 4Dy_3^2 + 12$. It follows that $4Dy_3^2 = 0$, which is impossible. If $t > 1$, again from (11) we see that $9|3x_3^2$, which is also impossible. We have shown that $r = 1$. If $q > 3$, we claim that $P_q \neq p^n$. Otherwise, $q \equiv 1 \pmod 4$. We write $q = 4k+1$. As

$$P_q = P_{4k+1} = (P_{2k+1} - P_{2k})(P_{2k+1} + P_{2k}),$$

$$((P_{2k+1}-P_{2k}),(P_{2k+1}+P_{2k}))=1,$$

and

$$((P_{2k+1}-P_{2k}),(P_{2k+1}+P_{2k}))|2(P_{2k},P_{2k+1})=2,\ 2\nmid P_q,$$

we have $P_{2k+1}-P_{2k}=1$. This is impossible. If $q\equiv 3 \pmod 4$, we write $q=4k+3$. From

$$P_q=P_{4k+3}=(P_{2k+2}-P_{2k+1})(P_{2k+2}+P_{2k+1}),$$
$$((P_{2k+2}-P_{2k+1}),(P_{2k+2}+P_{2k+1}))=1$$

and as

$$((P_{2k+2}-P_{2k+1}),(P_{2k+2}+P_{2k+1}))|2(P_{2k+2},P_{2k+1})=2, 2\nmid P_q,$$

we obtain $P_{2k+2}-P_{2k+1}=1$, which is also impossible. Let $P\neq p$ be an arbitrary prime divisor of P_q. Then from equation (10), we can easily prove that $P=q$ and

$$q^2\nmid P_q.$$

Thus we have shown that $P_q=qp^n$ if $q>3$. On the other hand, if $q>5$, then when $q\equiv 1 \pmod 4$, we write $q=4k+1$. We have $k>2$ and $P_{2k+1}-P_{2k}=q$ or $P_{2k+1}+P_{2k}=q$. But $P_s=x_1P_{s-1}-P_{s-2}$, for $s\geq 2$. Hence we get $P_s-P_{s-1}=(x_1-1)P_{s-1}-P_{s-2}>2(P_{s-1}-P_{s-2})$, for $s\geq 3$. Thus we have $P_{2k+1}-P_{2k}>2^{2k}=4^k>4k+1=q$, for $k\geq 3$. This leads to a contradiction. When $q\equiv 3 \pmod 4$, we write $q=4k+3$. We have $k\geq 1$ and $P_{2k+2}-P_{2k+1}=q$ or $P_{2k+2}+P_{2k+1}=q$. But $P_{2k++2}-P_{2k=1}>2^{2k+1}>4k+3=q$, for $k\geq 1$. This also leads to a contradiction. Therefore, we have shown that $q=3$ or $q=5$. If $q=5$, by what we proved before we have $P_3-P_2=5$. Since $P_0=0,P_1=1,P_2=x_1,P_3=x_1^2-1$, we obtain $x_1(x_1-1)=6$. Thus $x_1=3$. From $x_1^2-Dy_1^2=4$, we get $Dy_1^2=5$. It follows that $D=5,y_1=1$. Therefore, $y=y_5=P_5=(P_3-P_2)(P_3+P_2)=(8-3)(8+3)=55$. This completes the proof. □

Remark 14. Again here, a similar result was obtained by A. Grelak and A. Grytczuk [7]. But we prove the above result, which gives explicit details on different possible cases useful for the proof of Theorem 3.

Finally, we recall the following result.

Theorem 15. ([19]) *Let $D\neq 2$ be a given positive nonsquare integer with $8\nmid D$.*
(i) *If $2|D$, then the following equation*

$$kx^2-ly^2=1, \tag{12}$$

has integer solutions, where k,l are such that $k>1,\ kl=D$.
(ii) *If $2\nmid D$, then there is one and only one of the following equations*

$$kx^2-ly^2=1,\ kx^2-ly^2=2 \tag{13}$$

which has integer solutions, where k, l are such that $k > 1$, $kl = D$ for the first equation and k, l are such that $k > 0$, $kl = D$ for the second equation.
(iii) *If $2 \nmid D$ and the equation $x^2 - Dy^2 = 4$ has solutions in odd integers x and y, then there is at least one (k, l) with $k > 1$, $kl = D$ such that the following equation*

$$kx^2 - ly^2 = 4 \tag{14}$$

has integer solutions.

3. Proofs of the Main Results

3.1. Proof of Theorem 2

Let

$$l = p^{a-b}k_1^{t_1-r_1} \cdots k_s^{t_s-r_s},\ D = l(ly^2 - \delta),\ z = p^b k_1^{r_1} \cdots k_s^{r_s}.$$

From (2), one can see that (x, z) is a solution of the equation

$$X^2 - DY^2 = 1. \tag{15}$$

(i) Since $(y, 1)$ is the minimal positive solution of the equation

$$lX^2 - (ly^2 - \delta)Y^2 = \delta,$$

we have that $(y\sqrt{l}+\sqrt{ly^2-\delta})^2/2 = ly^2-(\delta/2)+y\sqrt{l(ly^2-\delta)}$ gives the fundamental solution of (15). By Theorems 8 and 11, we have

$$x = ly^2 - \delta/2,\ z = y, \tag{16}$$

or

$$x = (ly^2 - \delta/2)^2 + l(ly^2 - \delta)y^2,\ z = 2y(ly^2 - \delta/2), \tag{17}$$

or

$$x = (ly^2-\delta/2)^3+3(ly^2-\delta/2)l(ly^2-\delta)y^2,\ z/y = (2ly^2-\delta)^2-1 = 3^t p^b, a = b. \tag{18}$$

It is easy to see that (17) is impossible since z is an odd integer. From (16), we have $p \mid y$ and

$$x = p^{a+b}k_1^{t_1+r_1} \cdots k_s^{t_s+r_s} - \frac{\delta}{2}, y = p^b k_1^{r_1} \cdots k_s^{r_s}.$$

If (18) is true, then $3^t y = k_1^{r_1} \cdots k_s^{r_s}$. It follows that $y = 3^{-t}k_1^{r_1} \cdots k_s^{r_s}$. If $\delta = 2$, again from (18), we obtain $2ly^2-3 = 3^t, 2ly^2-1 = p^b$. We get $2 \nmid t$ by considerations modulo 4. Therefore we have

$$p^b = 3^t + 2 = 2 \cdot 3^{-2t}k_1^{t_1+r_1} \cdots k_s^{t_s+r_s} - 1,\ x = \frac{1}{2}(p^b - 1)((p^b - 1)^2 - 3).$$

If $\delta = -2$, also from (18), we see that $2ly^2 + 3 = 3^t,\ 2ly^2 + 1 = p^b$. We get $2|t$ by considerations modulo 4. Therefore we have

$$p^b = 3^t - 2 = 2 \cdot 3^{-2t} k_1^{t_1+r_1} \cdots k_s^{t_s+r_s} + 1,\ x = \frac{1}{2}(p^b+1)((p^b+1)^2 - 3).$$

This proves (i) of Theorem 2.

(ii) Since $(y, 1)$ is a positive integer solution of the equation

$$lX^2 - (ly^2 - \delta)Y^2 = \delta,$$

we have that

$$u\sqrt{l} + v\sqrt{ly^2 - \delta} = ((y\sqrt{l} + v\sqrt{ly^2 - \delta})/2)^3$$

gives a solution of the equation $lX^2 - (ly^2 - \delta)Y^2 = \pm 1$. On the other hand, if (2) is true, note that $2 \nmid Dz^2$ and from (15) we get

$$x + 1 = D_1 z_1^2, x - 1 = D_2 z_2^2, D_1 D_2 = D, z = z_1 z_2.$$

Thus (z_1, z_2) is a solution of $D_1 X^2 - D_2 Y^2 = 2$, contradicting Theorem 15. This completes the proof of Theorem 2.

3.2. Proof of Theorem 3

Let

$$l = p^{a-b} k_1^{t_1-r_1} \cdots k_s^{t_s-r_s},\ D = l(ly^2 - \delta),\ z = p^b k_1^{r_1} \cdots k_s^{r_s}.$$

From Equation (3), one sees that (x, z) is a solution of the equation

$$X^2 - DY^2 = 4. \tag{19}$$

Since $(y, 1)$ is the minimal solution of the equation

$$lX^2 - (ly^2 - \delta)Y^2 = \delta,$$

$(y\sqrt{l} + \sqrt{ly^2 - \delta})^2/2 = ly^2 - (\delta/2) + y\sqrt{l(ly^2 - \delta)}$ gives the fundamental solution of (19). Using Theorems 9, 13 and Proposition 6, we have

$$x = ly^2 - \delta/2,\ z = y, \tag{20}$$

or

$$x = ((ly^2 - \delta/2)^2 + l(ly^2 - \delta)y^2)/2,\ z = y(ly^2 - \delta/2),\ a = b, \tag{21}$$

or

$$x = 123,\ D = 5,\ p^b k_1^{r_1} \cdots k_s^{r_s} = 55,\ a = b. \tag{22}$$

From Equation (20), we obtain $p|y$ and

$$x = p^{a+b}k_1^{t_1+r_1}\cdots k_s^{t_s+r_s} - \frac{\delta}{2},\ y = p^b k_1^{r_1}\cdots k_s^{r_s}.$$

Using (21), one can see that $p \nmid y$ and

$$p^b = k_1^{t_1+r_1}\cdots k_s^{t_s+r_s} - \frac{\delta}{2},\ x = p^{2b} - 2,\ y = k_1^{r_1}\cdots k_s^{r_s},\ a = b.$$

If (22) is true, we can easily see that

$$y = 1, p = 11, s = 1, r_1 = 1, t_1 = 2, k_1 = 5, a = b = 1, \delta = 4.$$

This completes the proof of Theorem 3.

Acknowledgments The authors express their gratitude to the anonymous referee for carefully examining this paper and providing a number of important comments and suggestions. The first and third authors are supported by the Guangdong Provincial Natural Science Foundation (No. 8151027501000114, 10152606101000000) and NSF of China (No. 10571180). The work on this paper was completed during a very enjoyable visit of the second author at *l'Institut de Mathématiques de Bordeaux*. He thanks the people of this institution for their hospitality. He is also partially supported by Purdue University North Central.

References

[1] Z. F. Cao, *A kind of Diophantine equation in finite simple groups*, (In Chinese), Northeast Math. J., **16** (4) (2000), 391–397.

[2] Z. F. Cao, A. Grytczuk, *Some classes of Diophantine equations connected with McFarland's conjecture*, Discuss Math-General Algebra and Applications, **20** (2) (2000), 49–62.

[3] L. E. Dickson, *History of the Theory of Numbers*, Vol.II, p. 36, Carnegie Inst., Washington, D. C. 1920.

[4] X. L. Dong, Z. F. Cao, *Generalization of a Diophantine equation in difference sets*, (In Chinese), J. Heilongqiang University, **19** (2) (2002), 1–4.

[5] Yongdong Guo, *On the exponential Diophaantine equation* $x^2 = 2^{2a}k^{2m} - 2^{2a}k^{m+n} + 1$, Discuss Math Algebra stokastic Methods, **16** (1) (1996), 57–60.

[6] A. Grelak, A. Grytczuk, *Some remarks on matrices and Diophaantine equation* $Ax^2 - By^2 = C$, Discuss. Math., **10** (1990), 13–27.

[7] A. Grelak, A. Grytczuk, *On the Diophaantine equation* $ax^2 - by^2 = c$, Publ. Math. Debrecen, **44** (1994), 291–299.

[8] M. Le, Q. Xiang, *A Result on Ma's Conjecture*, J. Combin. Theory Ser. A, **73** (1996), no.1, 181–184.

[9] D. H. Lehmer, *An extended theory of Lucas' functions*, Ann. Math., **31** (1930), 419–448.

[10] Jiagui Luo, *Extensions and applications of Störmer Theorem*, (in Chinese), J. Sichuan University, **28** (4) (1991), 469–474.

[11] J. Luo, P. Yuan, *Square-classes in Lehmer sequences having odd parameters and their applications*, Acta Arith., **127** (1) (2007), 49–62.

[12] H. Mei, L. Mei, Q. fan, W. Song, *Extensions of Störmer Theorem* (in Chinese), J. Yuzhou University, **12** (4) (1995), 25–27.

[13] S. L. Ma, *MaFarland's conjecture on Abelian difference sets with multiplier* -1, Designs, Codes and Cryptography, **1** (1992), 321–332.

[14] P. Ribenboim, *The Book of Prime Number Records*, Springer-Verlag, New York, (1989).

[15] Q. Sun and Pingzhi Yuan, *On the Diophantine equatins* $(ax^n-1)/(ax-1) = y^2$ *and* $(ax^n+1)/(ax+1) = y^2$ (In Chinese), J. Sichuan University (in Chinese), (1989), 20–24.

[16] D. T. Walker, *On the diophantine equation* $mX^2 - nY^2 = \pm 1$, Amer. Math. Monthly **74** (1967), 504-513.

[17] P. Yuan, *On the number of solutions of* $x^2 - 4m(m+1)y^2 = y^2 - bz^2 = 1$, Proc. Amer. Math. Soc **132** (2004), 1561–1566.

[18] Pingzhi Yuan, *A note on the divisibility of the generalized Lucas' sequences*, Fibonacci Quart., **2** (40) (2002), 153–156.

[19] Pingzhi Yuan, *A new proposition of Pell equation and its applications*, (in Chinese), J. Changsha Railway University, **12** (1994), 79–84.

[20] P. Yuan and J. Luo, *On solutions of higher degree diophantine equation*, (in Chinese), J. Math. Res. & Expo., **21** (1) (2001), 99–102.