Quadratic Diophantine Equation<br>$x^{2}-\left(t^{2}-t\right) y^{2}-(4 t-2) x+\left(4 t^{2}-4 t\right) y=0$<br>${ }^{1}$ Arzu Özkoç and ${ }^{2}$ Ahmet Tekcan<br>${ }^{1,2}$ Uludag University, Faculty of Science, Department of Mathematics, Görükle, 16059, Bursa-Turkey<br>${ }^{1}$ arzuozkoc@uludag.edu.tr, ${ }^{2}$ tekcan@uludag.edu.tr


#### Abstract

Let $t \geq 2$ be an integer. In this work, we consider the number of integer solutions of Diophantine equation $D: x^{2}-\left(t^{2}-t\right) y^{2}-(4 t-2) x+$ $\left(4 t^{2}-4 t\right) y=0$ over $\mathbb{Z}$. We also derive some recurrence relations on the integer solutions $\left(x_{n}, y_{n}\right)$ of $D$. In the last section, we consider the same problem over finite fields $\mathbb{F}_{p}$ for primes $p \geq 5$.


2000 Mathematics Subject Classification: 11D09, 11D79
Key words and phrases: Diophantine equation, Pell equation.

## 1. Introduction

A Diophantine equation is an indeterminate polynomial equation that allows the variables to be integers only. In more technical language, they define an algebraic curve, algebraic surface or more general object, and ask about the lattice points on it. The word Diophantine refers to the Hellenistic mathematician of the $3^{\text {rd }}$ century, Diophantus of Alexandria, who made a study of such equations and was one of the first mathematicians to introduce symbolism into algebra. In general, the Diophantine equation is the equation given by

$$
\begin{equation*}
a x^{2}+b x y+c y^{2}+d x+e y+f=0 \tag{1.1}
\end{equation*}
$$

Also the Diophantine equation

$$
\begin{equation*}
x^{2}-d y^{2}=1 \tag{1.2}
\end{equation*}
$$

which is a special case of (1.1), known as the Pell equation (see [3,14]), which is named after an English mathematician, John Pell, who searched for integer solutions to equations of this type in the seventeenth century. The Pell equation in (1.2) has infinitely many integer solutions $\left(x_{n}, y_{n}\right)$ for $n \geq 1$. The first positive integer solution $\left(x_{1}, y_{1}\right)$ of this equation is called the fundamental solution, because all other solutions can be (easily) derived from it. In fact, if $\left(x_{1}, y_{1}\right)$ is the fundamental

[^0]solution, then the $n$-th positive solution of it, say $\left(x_{n}, y_{n}\right)$, is defined by the equality $x_{n}+y_{n} \sqrt{d}=\left(x_{1}+y_{1} \sqrt{d}\right)^{n}$ for integer $n \geq 2$. There are several methods for finding the fundamental solution of $x^{2}-d y^{2}=1$. For example, the cyclic method known in India in the $12^{\text {th }}$ century, and the slightly less efficient but more regular English method in the $17^{\text {th }}$ century, produce all solutions of $x^{2}-d y^{2}=1$ (see [4]). But the most efficient method for finding the fundamental solution is based on the simple finite continued fraction expansion of $\sqrt{d}$ (see $[2,5,6,10,11]$ ). The Pell equation was first studied by Brahmagupta (598-670) and Bhaskara (1114-1185) (see [1]). Its complete theory was worked out by Lagrange (1736-1813), not Pell. It is often said that Euler (1707-1783) mistakenly attributed Brouncker's (1620-1684) work on this equation to Pell. However the equation appears in a book by Rahn (1622-1676) which was certainly written with Pell's help: Some say entirely written by Pell. Perhaps Euler knew what he was doing in naming the equation (for further details on Pell and Diophantine equations see $[7-9,12,13,15]$ ).
2. The Diophantine Equation $x^{2}-\left(t^{2}-t\right) y^{2}-(4 t-2) x+\left(4 t^{2}-4 t\right) y=0$

In [16-20], we considered some specific Pell (also Diophantine) equations and their integer solutions. In the present paper, we consider the integer solutions of Diophantine equation

$$
\begin{equation*}
D: x^{2}-\left(t^{2}-t\right) y^{2}-(4 t-2) x+\left(4 t^{2}-4 t\right) y=0 \tag{2.1}
\end{equation*}
$$

over $\mathbb{Z}$, where $t \geq 2$ is an integer. Note that it is very difficult to solve $D$ in its present form, that is, we can not determine how many integer solutions $D$ has and what they are. So we have to transform $D$ into an appropriate Diophantine equation which can be easily solved. To get this let

$$
T:\left\{\begin{array}{l}
x=u+h  \tag{2.2}\\
y=v+k
\end{array}\right.
$$

be a translation for some $h$ and $k$. In this case the pair $\{h, k\}$ is called the base of $T$ and denote it by $T[h ; k]=\{h, k\}$. If we apply $T$ to $D$, then we get

$$
\begin{equation*}
T(D)=\widetilde{D}:(u+h)^{2}-\left(t^{2}-t\right)(v+k)^{2}-(4 t-2)(u+h)+\left(4 t^{2}-4 t\right)(v+k)=0 \tag{2.3}
\end{equation*}
$$

In (2.3), we obtain $u(2 h-2-4 t)$ and $v\left(-2 k t^{2}-2 k t+4 t^{2}+4 t\right)$. So we get $h=2 t-1$ and $k=2$. Consequently for $x=u+2 t-1$ and $y=v+2$, we have the Diophantine equation

$$
\begin{equation*}
\widetilde{D}: u^{2}-\left(t^{2}-t\right) v^{2}=1 \tag{2.4}
\end{equation*}
$$

which is a Pell equation. Now we try to find all integer solutions $\left(u_{n}, v_{n}\right)$ of $\widetilde{D}$ and then we can retransfer all results from $\widetilde{D}$ to $D$ by using the inverse of $T$.
Theorem 2.1. Let $\widetilde{D}$ be the Diophantine equation in (2.4). Then
(1) The continued fraction expansion of $\sqrt{t^{2}-t}$ is

$$
\sqrt{t^{2}-t}= \begin{cases}{[1 ; \overline{2}]} & \text { if } t=2 \\ {[t-1 ; \overline{2,2 t-2}]} & \text { if } t>2\end{cases}
$$

(2) The fundamental solution of $\widetilde{D}$ is $\left(u_{1}, v_{1}\right)=(2 t-1,2)$.
(3) Define the sequence $\left\{\left(u_{n}, v_{n}\right)\right\}$, where

$$
\binom{u_{n}}{v_{n}}=\left(\begin{array}{cc}
2 t-1 & 2 t^{2}-2 t  \tag{2.5}\\
2 & 2 t-1
\end{array}\right)^{n}\binom{1}{0}
$$

for $n \geq 1$. Then $\left(u_{n}, v_{n}\right)$ is a solution of $\widetilde{D}$.
(4) The solutions $\left(u_{n}, v_{n}\right)$ satisfy $u_{n}=(2 t-1) u_{n-1}+\left(2 t^{2}-2 t\right) v_{n-1}$ and $v_{n}=$ $2 u_{n-1}+(2 t-1) v_{n-1}$ for $n \geq 2$.
(5) The solutions $\left(u_{n}, v_{n}\right)$ satisfy the recurrence relations $u_{n}=(4 t-3)\left(u_{n-1}+\right.$ $\left.u_{n-2}\right)-u_{n-3}$ and $v_{n}=(4 t-3)\left(v_{n-1}+v_{n-2}\right)-v_{n-3}$ for $n \geq 4$.
(6) The $n$-th solution $\left(u_{n}, v_{n}\right)$ can be given by

$$
\begin{equation*}
\frac{u_{n}}{v_{n}}=[t-1 ; \underbrace{2,2 t-2, \cdots, 2,2 t-2}_{n-1 \text { times }}, 2] \tag{2.6}
\end{equation*}
$$

for $n \geq 1$.
Proof.
(1) Let $t=2$. Then it is easily seen that $\sqrt{2}=[1 ; \overline{2}]$. Now let $t>2$. Then

$$
\begin{aligned}
\sqrt{t^{2}-t} & =t-1+\left(\sqrt{t^{2}-t}-t+1\right)=t-1+\frac{1}{\frac{\sqrt{t^{2}-t}+t-1}{t-1}} \\
& =t-1+\frac{1}{2+\frac{\sqrt{t^{2}-t}-t+1}{t-1}}=t-1+\frac{1}{2+\frac{1}{\sqrt{t^{2}-t}+t-1}} \\
& =t-1+\frac{1}{2+\frac{1}{2 t-2+\left(\sqrt{t^{2}-t}-t+1\right)}}
\end{aligned}
$$

So $\sqrt{t^{2}-t}=[t-1 ; \overline{2,2 t-2}]$.
(2) It is easily seen that $\left(u_{1}, v_{1}\right)=(2 t-1,2)$ is the fundamental solution of $\widetilde{D}$ since $(2 t-1)^{2}-\left(t^{2}-t\right) 2^{2}=1$.
(3) We prove it by induction. Let $n=1$. Then by (2.5), we get $\left(u_{1}, v_{1}\right)=$ $(2 t-1,2)$ which is the fundamental solution and so is a solution of $\widetilde{D}$. Let us assume that the Diophantine equation in (2.4) is satisfied for $n-1$, that is, $\widetilde{D}: u_{n-1}^{2}-\left(t^{2}-t\right) v_{n-1}^{2}=1$. We want to show that this equation is also satisfied for $n$. Applying (2.5), we find that

$$
\begin{aligned}
\binom{u_{n}}{v_{n}} & =\left(\begin{array}{cc}
2 t-1 & 2 t^{2}-2 t \\
2 & 2 t-1
\end{array}\right)^{n}\binom{1}{0} \\
& =\left(\begin{array}{cc}
2 t-1 & 2 t^{2}-2 t \\
2 & 2 t-1
\end{array}\right)\left(\begin{array}{cc}
2 t-1 & 2 t^{2}-2 t \\
2 & 2 t-1
\end{array}\right)^{n-1}\binom{1}{0} \\
& =\left(\begin{array}{cc}
2 t-1 & 2 t^{2}-2 t \\
2 & 2 t-1
\end{array}\right)\binom{u_{n-1}}{v_{n-1}} \\
& =\binom{(2 t-1) u_{n-1}+\left(2 t^{2}-2 t\right) v_{n-1}}{2 u_{n-1}+(2 t-1) v_{n-1}} .
\end{aligned}
$$

Hence we conclude that

$$
\begin{aligned}
u_{n}^{2}-\left(t^{2}-t\right) v_{n}^{2}= & \left((2 t-1) u_{n-1}+\left(2 t^{2}-2 t\right) v_{n-1}\right)^{2} \\
& -\left(t^{2}-t\right)\left(2 u_{n-1}+(2 t-1) v_{n-1}\right)^{2} \\
= & u_{n-1}^{2}-\left(t^{2}-t\right) v_{n-1}^{2}=1
\end{aligned}
$$

So $\left(u_{n}, v_{n}\right)$ is also a solution of $\widetilde{D}$.
(4) From (2.7), we find that $u_{n}=(2 t-1) u_{n-1}+\left(2 t^{2}-2 t\right) v_{n-1}$ and $v_{n}=$ $2 u_{n-1}+(2 t-1) v_{n-1}$ for $n \geq 2$.
(5) We only prove that $u_{n}$ satisfy the recurrence relation. For $n=4$, we get $u_{1}=2 t-1, u_{2}=8 t^{2}-8 t+1, u_{3}=32 t^{3}-48 t^{2}+18 t-1$ and $u_{4}=$ $128 t^{4}-256 t^{3}+160 t^{2}-32 t+1$. Hence

$$
\begin{aligned}
u_{4} & =(4 t-3)\left(u_{3}+u_{2}\right)-u_{1} \\
& =(4 t-3)\left(32 t^{3}-40 t^{2}+10 t\right)-(2 t-1) \\
& =128 t^{4}-256 t^{3}+160 t^{2}-32 t+1 .
\end{aligned}
$$

So $u_{n}=(4 t-3)\left(u_{n-1}+u_{n-2}\right)-u_{n-3}$ is satisfied for $n=4$. Let us assume that this relation is satisfied for $n-1$, that is,

$$
\begin{equation*}
u_{n-1}=(4 t-3)\left(u_{n-2}+u_{n-3}\right)-u_{n-4} . \tag{2.8}
\end{equation*}
$$

Then applying the previous assertion, (2.7) and (2.8), we conclude that $u_{n}=(4 t-3)\left(u_{n-1}+u_{n-2}\right)-u_{n-3}$ for $n \geq 4$.
(6) Note that

$$
\frac{u_{1}}{v_{1}}=[t-1 ; 2]=t-1+\frac{1}{2}=\frac{2 t-1}{2}
$$

which is the fundamental solution. Let us assume that $\left(u_{n}, v_{n}\right)$ is a solution of $\widetilde{D}$, that is, $u_{n}^{2}-\left(t^{2}-t\right) v_{n}^{2}=1$. Then by (2.6), we derive

$$
\begin{aligned}
\frac{u_{n+1}}{v_{n+1}} & =t-1+\frac{1}{2+\frac{1}{2 t-2+\frac{1}{2+\frac{1}{2 t-2+\frac{1}{\cdot+2 t-2+\frac{1}{2}}}}}} \\
& =t-1+\frac{1}{2+\frac{1}{t-1+t-1+\frac{1}{2+\frac{1}{2 t-2+\frac{1}{\cdot+2 t-2+\frac{1}{2}}}}}} \\
& =t-1+\frac{1}{2+\frac{1}{t-1+\frac{u_{n}}{v_{n}}}}=\frac{(2 t-1) u_{n}+\left(2 t^{2}-2 t\right) v_{n}}{2 u_{n}+(2 t-1) v_{n}} .
\end{aligned}
$$

So $\left(u_{n+1}, v_{n+1}\right)$ is also a solution of $\widetilde{D}$ since

$$
\begin{aligned}
u_{n+1}^{2}-\left(t^{2}-t\right) v_{n+1}^{2} & =\left((2 t-1) u_{n}+\left(2 t^{2}-2 t\right) v_{n}\right)^{2}-\left(t^{2}-t\right)\left(2 u_{n}+(2 t-1) v_{n}\right)^{2} \\
& =u_{n}^{2}-\left(t^{2}-t\right) v_{n}^{2}=1
\end{aligned}
$$

This completes the proof.

Example 2.1. Let $t=4$. Then $\left(u_{1}, v_{1}\right)=(7,2)$ is the fundamental solution of $\widetilde{D}: u^{2}-12 v^{2}=1$ and some other solutions are

$$
\begin{aligned}
& \binom{u_{2}}{v_{2}}=\left(\begin{array}{cc}
7 & 24 \\
2 & 7
\end{array}\right)^{2}\binom{1}{0}=\binom{97}{28} \\
& \binom{u_{3}}{v_{3}}=\left(\begin{array}{cc}
7 & 24 \\
2 & 7
\end{array}\right)^{3}\binom{1}{0}=\binom{1351}{390} \\
& \binom{u_{4}}{v_{4}}=\left(\begin{array}{cc}
7 & 24 \\
2 & 7
\end{array}\right)^{4}\binom{1}{0}=\binom{18817}{5432} \\
& \binom{u_{5}}{v_{5}}=\left(\begin{array}{cc}
7 & 24 \\
2 & 7
\end{array}\right)^{5}\binom{1}{0}=\binom{262087}{75658} \\
& \binom{u_{6}}{v_{6}}=\left(\begin{array}{cc}
7 & 24 \\
2 & 7
\end{array}\right)^{6}\binom{1}{0}=\binom{3650401}{1053780} .
\end{aligned}
$$

Also $u_{n}=7 u_{n-1}+24 v_{n-1}$ and $v_{n}=2 u_{n-1}+7 v_{n-1}$ for $n \geq 2 ; u_{n}=13\left(u_{n-1}+\right.$ $\left.u_{n-2}\right)-u_{n-3}$ and $v_{n}=13\left(v_{n-1}+v_{n-2}\right)-v_{n-3}$ for $n \geq 4$. Further

$$
\begin{aligned}
& \frac{u_{2}}{v_{2}}=[3 ; 2,6,2]=\frac{97}{28} \\
& \frac{u_{3}}{v_{3}}=[3 ; 2,6,2,6,2]=\frac{1351}{390} \\
& \frac{u_{4}}{v_{4}}=[3 ; 2,6,2,6,2,6,2]=\frac{18817}{5432} \\
& \frac{u_{5}}{v_{5}}=[3 ; 2,6,2,6,2,6,2,6,2]=\frac{262087}{75658} \\
& \frac{u_{6}}{v_{6}}=[3 ; 2,6,2,6,2,6,2,6,2,6,2]=\frac{3650401}{1053780} .
\end{aligned}
$$

From above theorem we can give the following result.
Corollary 2.1. The base of the transformation $T$ in (2.2) is the fundamental solution of $\widetilde{D}$, that is $T[h ; k]=\{h, k\}=\left\{u_{1}, v_{1}\right\}$.

Proof. We proved that $\left(u_{1}, v_{1}\right)=(2 t-1,2)$ is the fundamental solution of $\widetilde{D}$. Also we showed that $h=2 t-1$ and $k=2$. So the base of $T$ is $T[h ; k]=\{h, k\}=\{2 t-1,2\}$ as we claimed.

We saw as above that the Diophantine equation $D$ could be transformed into the Diophantine equation $\widetilde{D}$ via the transformation $T$. Also we showed that $x=u+2 t$ -1 and $y=v+2$. So we can retransfer all results from $\widetilde{D}$ to $D$ by using the inverse of $T$. Thus we can give the following main theorem.

Theorem 2.2. Let $D$ be the Diophantine equation in (2.1). Then
(1) The fundamental (minimal) solution of $D$ is $\left(x_{1}, y_{1}\right)=(4 t-2,4)$.
(2) Define the sequence $\left\{\left(x_{n}, y_{n}\right)\right\}_{n \geq 1}=\left\{\left(u_{n}+2 t-1, v_{n}+2\right)\right\}$, where $\left\{\left(u_{n}, v_{n}\right)\right\}$ defined in (2.5). Then $\left(x_{n}, y_{n}\right)$ is a solution of $D$. So it has infinitely many many integer solutions $\left(x_{n}, y_{n}\right) \in \mathbb{Z} \times \mathbb{Z}$.
(3) The solutions $\left(x_{n}, y_{n}\right)$ satisfy

$$
\begin{aligned}
& x_{n}=(2 t-1) x_{n-1}+\left(2 t^{2}-2 t\right) y_{n-1}-8 t^{2}+10 t-2 \\
& y_{n}=2 x_{n-1}+(2 t-1) y_{n-1}-8 t+6
\end{aligned}
$$

for $n \geq 2$.
(4) The solutions $\left(x_{n}, y_{n}\right)$ satisfy the recurrence relations

$$
\begin{aligned}
& x_{n}=(4 t-3)\left(x_{n-1}+x_{n-2}\right)-x_{n-3}-16 t^{2}+24 t-8 \\
& y_{n}=(4 t-3)\left(y_{n-1}+y_{n-2}\right)-y_{n-3}-16 t+16
\end{aligned}
$$

for $n \geq 4$.

## 3. The Diophantine Equation $x^{2}-\left(t^{2}-t\right) y^{2}-(4 t-2) x+\left(4 t^{2}-4 t\right) y=0$ over finite fields

In this section, we will consider the integer solutions of $D$ over finite fields $\mathbb{F}_{p}$ for primes $p \geq 5$. Let $t \in \mathbb{F}_{p}^{*}$ and let $t^{2}-t \equiv d(\bmod p)$. Then $\widetilde{D}$ becomes

$$
\begin{equation*}
\widetilde{D}_{p}^{d}: u^{2}-d v^{2} \equiv 1(\bmod p) \tag{3.1}
\end{equation*}
$$

Let $\widetilde{D}_{p}^{d}\left(\mathbb{F}_{p}\right)=\left\{(u, v) \in \mathbb{F}_{p} \times \mathbb{F}_{p}: u^{2}-d v^{2} \equiv 1(\bmod p)\right\}$. Then we can give the following theorem.

Theorem 3.1. Let $\widetilde{D}_{p}^{d}$ be the Diophantine equation in (3.1). Then

$$
\# \widetilde{D}_{p}^{d}\left(\mathbb{F}_{p}\right)= \begin{cases}p-1 & \text { for } d \in Q_{p} \\ p+1 & \text { for } d \notin Q_{p}\end{cases}
$$

where $Q_{p}$ denote the set of quadratic residues.
Proof. Let $d \in Q_{p}$ and let $p \equiv 1,5(\bmod 8)$. If $v=0$, then $u^{2} \equiv 1(\bmod p) \Leftrightarrow u \equiv$ $\pm 1(\bmod p)$. So $\widetilde{D}_{p}^{d}$ has two integer solutions $(1,0)$ and $(p-1,0)$. If $u=0$, then $-d v^{2} \equiv 1(\bmod p)$ has two solutions $v_{1}, v_{2}$. So $\widetilde{D}_{p}^{d}$ has two integer solutions $\left(0, v_{1}\right)$ and $\left(0, v_{2}\right)$. Now let $S_{p}=\mathbb{F}_{p}^{*}-\{1, p-1\}$. Then there are $(p-5) / 2$ points $u$ in $S_{p}$ such that $\left(u^{2}-1\right) / d$ is a square. Set $\left(u^{2}-1\right) / d=c^{2}$ for some $c \neq 0$. Then $v^{2} \equiv c^{2}(\bmod p) \Leftrightarrow v \equiv \pm c(\bmod p)$. So $\widetilde{D}_{p}^{d}$ has two solutions $(u, c)$ and $(u,-c)$, that is, for each $u$ in $S_{p}, \widetilde{D}_{p}^{d}$ has two solutions. So it has $2((p-5) / 2)=p-5$ solutions. We see as above that it has also four solutions $(1,0),(p-1,0),\left(0, v_{1}\right)$ and $\left(0, v_{2}\right)$. Therefore $\widetilde{D}_{p}^{d}$ has $p-5+4=p-1$ integer solutions. Now let $p \equiv 3,7(\bmod 8)$. If $v=0$, then $u^{2} \equiv 1(\bmod p)$ and hence $u=1$ and $u=p-1$. So $\widetilde{D}_{p}^{d}$ has two integer solutions $(1,0)$ and $(p-1,0)$. If $u=0$, then $-d v^{2} \equiv 1(\bmod p)$ has no solution. So $\widetilde{D}_{p}^{d}$ has no integer solution $(0, v)$. Let $H_{p}=\mathbb{F}_{p}^{*}-\{1, p-1\}$. Then there are $(p-3) / 2$ points $u$ in $H_{p}$ such that $\left(u^{2}-1\right) / d$ is a square. Set $\left(u^{2}-1\right) / d=j^{2}$ for some $j \neq 0$. Then $v^{2} \equiv j^{2}(\bmod p) \Leftrightarrow v \equiv \pm j(\bmod p)$. So $\widetilde{D}_{p}^{d}$ has two solutions $(u, j)$ and $(u,-j)$, that is, for each $u$ in $H_{p}, \widetilde{D}_{p}^{d}$ has two solutions. So it has $2((p-3) / 2)=p-3$ solutions. It has also two solutions $(1,0)$ and $(p-1,0)$. Therefore $\widetilde{D}_{p}^{d}$ has $p-3+2=p-1$ integer solutions.

Similarly it can be shown that if $d \notin Q_{p}$, then $\widetilde{D}_{p}^{d}$ has $p+1$ integer solutions.

Example 3.1. Let $t=4$. Then $12 \in Q_{23}$ and $12 \notin Q_{31}$. So

$$
\begin{aligned}
& \widetilde{D}_{23}^{12}\left(\mathbb{F}_{23}\right)=\left\{\begin{array}{c}
(1,0),(2,11),(2,12),(3,4),(3,19),(5,5),(5,18),(6,1),(6,22),(7,2), \\
(7,21),(16,2),(16,21),(17,1),(17,22),(18,5),(18,18),(20,4), \\
(20,19),(21,11),(21,12),(22,0)
\end{array}\right\} \\
& \widetilde{D}_{31}^{12}\left(\mathbb{F}_{31}\right)=\left\{\begin{array}{c}
(0,7),(0,24),(1,0),(2,15),(2,16),(4,3),(4,28),(5,8),(5,23),(7,2), \\
(7,29),(10,4),(10,27),(11,14),(11,17),(13,13),(13,18),(18,13), \\
(18,18),(20,14),(20,17),(21,4),(21,27),(24,2),(24,29),(26,8), \\
(26,23),(27,3),(27,28),(29,15),(29,16),(30,0)
\end{array}\right\} .
\end{aligned}
$$

For the Diophantine equation $D$, we set

$$
D\left(\mathbb{F}_{p}\right)=\left\{(x, y) \in \mathbb{F}_{p} \times \mathbb{F}_{p}: x^{2}-\left(t^{2}-t\right) y^{2}-(4 t-2) x+\left(4 t^{2}-4 t\right) y=0(\bmod p)\right\} .
$$

Then we can give the following theorem.
Theorem 3.2. Let $D$ be the Diophantine equation in (2.1). Then

$$
\# D\left(\mathbb{F}_{p}\right)= \begin{cases}p-1 & \text { for } t^{2}-t \in Q_{p} \\ p+1 & \text { for } t^{2}-t \notin Q_{p} .\end{cases}
$$

## References

[1] S. P. Arya, On the Brahmagupta-Bhaskara equation, Math. Ed. 8 (1991), no. 1, 23-27.
[2] C. Baltus, Continued fractions and the Pell equations. The work of Euler and Lagrange, Comm. Anal. Theory Contin. Fractions 3 (1994), 4-31.
[3] E. J. Barbeau, Pell's Equation, Springer, New York, 2003.
[4] H. P. Edward Fermat's Last Theorem. A Genetic Introduction to Algebraic Number Theory. Corrected reprint of the 1977 original. Graduate Texts in Mathematics, 50. Springer-Verlag, New York, 1996.
[5] D. Hensley, Continued Fractions, World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2006.
[6] P. Kaplan and K. S. Williams, Pell's equations $X^{2}-m Y^{2}=-1,-4$ and continued fractions, J. Number Theory 23 (1986), no. 2, 169-182.
[7] H. W. Lenstra, Jr., Solving the Pell equation, Notices Amer. Math. Soc. 49 (2002), no. 2, 182-192.
[8] K. Matthews, The Diophantine equation $x^{2}-D y^{2}=N, D>0$, Expo. Math. 18 (2000), no. 4, 323-331.
[9] R. A. Mollin, A. J. van der Poorten and H. C. Williams, Halfway to a solution of $X^{2}-D Y^{2}=$ -3, J. Théor. Nombres Bordeaux 6 (1994), no. 2, 421-457.
[10] R. A. Mollin, Simple continued fraction solutions for Diophantine equations, Expo. Math. 19 (2001), no. 1, 55-73.
[11] R. A. Mollin, The Diophantine equation $a x^{2}-b y^{2}=c$ and simple continued fractions, Int. Math. J. 2 (2002), no. 1, 1-6.
[12] R. A. Mollin, A note on the Diophantine equation $D_{1} x^{2}+D_{2}=a k^{n}$, Acta Math. Acad. Paedagog. Nyházi. (N.S.) 21 (2005), no. 1, 21-24 (electronic).
[13] R. A. Mollin, Quadratic Diophantine equations $x^{2}-D y^{2}=c^{n}$, Irish Math. Soc. Bull. 58 (2006), 55-68.
[14] I. Niven, H. S. Zuckerman and H. L. Montgomery, An Introduction to the Theory of Numbers, Fifth edition, Wiley, New York, 1991.
[15] P. Stevenhagen, A density conjecture for the negative Pell equation, in Computational Algebra and Number Theory (Sydney, 1992), 187-200, Kluwer Acad. Publ., Dordrecht.
[16] A. Tekcan, Pell equation $x^{2}-D y^{2}=2$. II, Irish Math. Soc. Bull. 54 (2004), 73-89.
[17] A. Tekcan, O. Bizim and M. Bayraktar, Solving the Pell equation using the fundamental element of the field $\mathbb{Q}(\sqrt{\Delta})$, Southeast Asian Bull. Math. 30 (2006), no. 2, 355-366.
[18] A. Tekcan, The Pell equation $x^{2}-D y^{2}= \pm 4$, Appl. Math. Sci. (Ruse) 1 (2007), no. 5-8, 363-369.
[19] A. Tekcan, B. Gezer and O. Bizim, On the integer solutions of the Pell equation $x^{2}-d y^{2}=2^{t}$, Int. J. Math. Sci. (WASET) 1 (2007), no. 3, 204-208 (electronic).
[20] A. Tekcan, The Diophantine equation $4 y^{2}-4 y x-1=0$, curves and conics over finite fields, accepted for publication in Mathematical Reports.


[^0]:    Communicated by Ang Miin Huey.
    Received: April 2, 2009; Revised: June 4, 2009.

