Rev Mat Complut (2010) 23: 251–260
DOI 10.1007/s13163-009-0009-8

# The Diophantine equation $x^2 - (t^2 + t)y^2 - (4t + 2)x + (4t^2 + 4t)y = 0$

**Ahmet Tekcan · Arzu Özkoç**

Received: 14 April 2009 / Accepted: 25 May 2009 / Published online: 5 November 2009

**Abstract** Let $t \geq 1$ be an integer. In this work, we consider the number of integer solutions of Diophantine equation

$$x^2 - (t^2 + t)y^2 - (4t + 2)x + (4t^2 + 4t)y = 0$$

over $\mathbb{Z}$ and also over finite fields $\mathbb{F}_p$ for primes $p \geq 5$.

**Keywords** Diophantine equation · Pell equation

**Mathematics Subject Classification (2000)** 11D09 · 11D41 · 11D45

## 1 Preliminaries

A Diophantine equation is an indeterminate polynomial equation that allows the variables to be integers only. Diophantine problems have fewer equations than unknown variables and involve finding integers that work correctly for all equations. 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 3rd century, Diophantus of Alexandria, who made a study of such equations and was one of the first mathematicians to introduce symbolism into algebra. The mathematical study of Diophantine problems Diophantus initiated is now called Diophantine analysis. A linear Diophantine equation is an

A. Tekcan (✉) · A. Özkoç
Faculty of Science, Department of Mathematics, Uludag University, Görükle, Bursa, Turkey
e-mail: tekcan@uludag.edu.tr
url: http://matematik.uludag.edu.tr/AhmetTekcan.htm

A. Özkoç
e-mail: arzuozkoc@uludag.edu.tr

equation between two sums of monomials of degree zero or one. While individual equations present a kind of puzzle and have been considered throughout history, the formulation of general theories of Diophantine equations was an achievement of the twentieth century. For example, the equation $ax + by = 1$ is known the linear Diophantine equation. In general, the Diophantine equation is the equation given by

$$ax^2 + bxy + cy^2 + dx + ey + f = 0. \tag{1.1}$$

Also for $n = 2$, there are infinitely many solutions $(x, y, z)$ of the Diophantine equation $x^n + y^n = z^n$. For larger values of $n$, Fermat's last theorem (see [4]) states that no positive integer solutions $x, y, z$ satisfying the equation exist. The Diophantine equation

$$x^2 - dy^2 = 1 \tag{1.2}$$

is known the Pell equation (see [3, 16]) which is named after the English mathematician John Pell a mathematician 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 $(x_n, y_n)$ for $n \geq 1$. The first non-trivial positive integer solution $(x_1, y_1)$ of this equation is called the fundamental solution, because all other solutions can be (easily) derived from it. In fact if $(x_1, y_1)$ is the fundamental solution, then the $n$-th positive solution of it, say $(x_n, y_n)$, is defined by the equality

$$x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n \tag{1.3}$$

for integer $n \geq 2$. There are several methods for finding the fundamental solution of $x^2 - dy^2 = 1$. For example, the cyclic method known in India in the 12th century, and the slightly less efficient but more regular English method 17th century, produce all solutions of $x^2 - dy^2 = 1$ (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, 10–13]). We can describe it as follows: Let $[a_0; \overline{a_1, \ldots, a_r, 2a_0}]$ be the simple continued fraction of $\sqrt{d}$ $(a_0 = \lfloor\sqrt{d}\rfloor)$. Let $p_0 = a_0$, $p_1 = 1 + a_0a_1$, $q_0 = 1$, $q_1 = a_1$, $p_n = a_np_{n-1} + p_{n-2}$ and $q_n = a_nq_{n-1} + q_{n-2}$ for $n \geq 2$. If $r$ is odd, then the fundamental solution is $(x_1, y_1) = (p_r, q_r)$, where $p_r/q_r$ is the $r$th convergent of $\sqrt{d}$ and if $r$ is even, then the fundamental solution is $(x_1, y_1) = (p_{2r+1}, q_{2r+1})$.

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. Baltus [2], Kaplan and Williams [6], Lenstra [7], Matthews [8], Mollin (also Poorten and Williams) [9, 14, 15], Stevenhagen [17], Tekcan [18–23], and the others considered some specific Pell (and Diophantine) equations and their integer solutions.

## 2 The Diophantine equation $x^2-(t^2+t)y^2-(4t+2)x+(4t^2+4t)y=0$

Let $t \geq 1$ be an integer. In this section, we will consider the integer solutions of Diophantine equation

$$D : x^2-(t^2+t)y^2-(4t+2)x+(4t^2+4t)y=0 \tag{2.1}$$

over $\mathbb{Z}$. (Note that $D$ has always two integer solutions $(0,0)$ and $(0,4)$ for every arbitrary $t \geq 1$. So we omit these two solutions.) Note that $D$ represents a conic. So before considering our main problem, we give some preliminaries on conics. Recall that a conic $C$ is given by an equation

$$C : ax^2+bxy+cy^2+dx+ey+f=0, \tag{2.2}$$

where $a,b,c,d,e$ and $f$ are real numbers. The discriminant of $C$ is $\Delta(C)=b^2-4ac$. If $\Delta(C)<0$, then $C$ represents an ellipse; $\Delta(C)>0$, then $C$ represents a hyperbole and if $\Delta(C)=0$, then $C$ represents a parabola. If $b=0$, then we can transform $C$ to a centripetal conic on the $uv$-plane via the transformation

$$T : \begin{cases} x=u+h, \\ y=v+k \end{cases} \tag{2.3}$$

for some $h$ and $k$. Here we call the pair $\{h,k\}$ as the base of $T$ and denote it by

$$T[h;k]=\{h,k\}. \tag{2.4}$$

Since a Diophantine equation $D$ represents a conic $C$, the corresponding conic is hence

$$C : x^2-(t^2+t)y^2-(4t+2)x+(4t^2+4t)y=0. \tag{2.5}$$

Now we want to carry out $C$ to a centripetal conic on $uv$-plane. To get this let $x=u+h$ and $y=v+k$ for some $h$ and $k$. Then (2.5) becomes

$$\widetilde{C} : (u+h)^2-(t^2+t)(v+k)^2-(4t+2)(u+h)+(4t^2+4t)(v+k)=0. \tag{2.6}$$

In (2.6), we obtain $u(2h-2-4t)$ and $v(-2kt^2-2kt+4t^2+4t)$. So we get

$$h=2t+1 \quad \text{and} \quad k=2 \tag{2.7}$$

since the coefficients $u$ and $v$ must be zero. Therefore for

$$x=u+2t+1 \quad \text{and} \quad y=v+2, \tag{2.8}$$

we get

$$\widetilde{C} : u^2-(t^2+t)v^2=1 \tag{2.9}$$

which is a centripetal conic (in fact a hyperbole) on $uv$-plane with focuses 1 and $\frac{1}{\sqrt{(t^2+t)}}$. So the corresponding Diophantine equation is hence

$$\widetilde{D} : u^2-(t^2+t)v^2=1. \tag{2.10}$$

In fact this a Pell equation by (1.2). Now we can consider the integer solutions of $\widetilde{D}$.

**Theorem 2.1** *Let $\widetilde{D}$ be the Diophantine equation in (2.10). Then*

(1) *The fundamental solution of $\widetilde{D}$ is $(u_1, v_1) = (2t+1, 2)$.*

(2) *Define the sequence $\{(u_n, v_n)\}$, where*

$$\begin{pmatrix} u_n \\ v_n \end{pmatrix} = \begin{pmatrix} 2t+1 & 2t^2+2t \\ 2 & 2t+1 \end{pmatrix}^n \begin{pmatrix} 1 \\ 0 \end{pmatrix} \tag{2.11}$$

*for $n \geq 1$. Then $(u_n, v_n)$ is a solution of $\widetilde{D}$.*

(3) *The solutions $(u_n, v_n)$ satisfy $u_n = (2t+1)u_{n-1} + (2t^2+2t)v_{n-1}$ and $v_n = 2u_{n-1} + (2t+1)v_{n-1}$ for $n \geq 2$.*

(4) *The solutions $(u_n, v_n)$ satisfy the recurrence relations $u_n = (4t+1)(u_{n-1} + u_{n-2}) - u_{n-3}$ and $v_n = (4t+1)(v_{n-1} + v_{n-2}) - v_{n-3}$ for $n \geq 4$.*

(5) *The continued fraction expansion of $\sqrt{t^2+t}$ is*

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

(6) *The $n$-th solution $(u_n, v_n)$ can be given by*

$$\frac{u_n}{v_n} = \Big[t; \underbrace{t, 2t, \ldots, t, 2t}_{n-1\, times}, 2\Big] \tag{2.12}$$

*for $n \geq 1$.*

*Proof* 1. It is easily seen that $(u_1, v_1) = (2t+1, 2)$ is the fundamental solution of $\widetilde{D}$ since $(2t+1)^2 - (t^2+t)2^2 = 1$.

2. We prove it by induction on $n$. Let $n = 1$. Then by (2.11), we get $(u_1, v_1) = (2t+1, 2)$ which is a solution of $\widetilde{D}$ since $(u_1, v_1)$ is the fundamental solution. Let us assume that the Diophantine equation in (2.10) is satisfied for $n-1$, that is,

$$\widetilde{D} : u_{n-1}^2 - (t^2+t)v_{n-1}^2 = 1. \tag{2.13}$$

We want to show that this equation is also satisfied for $n$. Applying (2.11), we find that

$$\begin{aligned} \begin{pmatrix} u_n \\ v_n \end{pmatrix} &= \begin{pmatrix} 2t+1 & 2t^2+2t \\ 2 & 2t+1 \end{pmatrix}^n \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ &= \begin{pmatrix} 2t+1 & 2t^2+2t \\ 2 & 2t+1 \end{pmatrix} \begin{pmatrix} 2t+1 & 2t^2+2t \\ 2 & 2t+1 \end{pmatrix}^{n-1} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ &= \begin{pmatrix} 2t+1 & 2t^2+2t \\ 2 & 2t+1 \end{pmatrix} \begin{pmatrix} u_{n-1} \\ v_{n-1} \end{pmatrix} \\ &= \begin{pmatrix} (2t+1)u_{n-1} + (2t^2+2t)v_{n-1} \\ 2u_{n-1} + (2t+1)v_{n-1} \end{pmatrix}. \end{aligned} \tag{2.14}$$

Hence we conclude that

$$\begin{aligned}
&u_n^2-(t^2+t)v_n^2\\
&\quad=\big((2t+1)u_{n-1}+(2t^2+2t)v_{n-1}\big)^2-(t^2+t)\big(2u_{n-1}+(2t+1)v_{n-1}\big)^2\\
&\quad=(2t+1)^2u_{n-1}^2+2(2t+1)(2t^2+2t)u_{n-1}v_{n-1}+(2t^2+2t)^2v_{n-1}^2\\
&\qquad-(t^2+t)\big(4u_{n-1}^2+4(2t+1)u_{n-1}v_{n-1}+(2t+1)^2v_{n-1}^2\big)\\
&\quad=u_{n-1}^2\big((2t+1)^2-4(t^2+t)\big)\\
&\qquad+u_{n-1}v_{n-1}\big(2(2t+1)(2t^2+2t)-(t^2+t)4(2t+1)\big)\\
&\qquad+v_{n-1}^2\big((2t^2+2t)^2-(t^2+t)(2t+1)^2\big)\\
&\quad=u_{n-1}^2-(t^2+t)v_{n-1}^2\\
&\quad=1
\end{aligned}$$

since $u_{n-1}^2-(t^2+t)v_{n-1}^2=1$ by (2.13). So $(u_n,v_n)$ is also a solution of $\widetilde{D}$.

3. Applying (2.14), we find that $u_n=(2t+1)u_{n-1}+(2t^2+2t)v_{n-1}$ and $v_n=2u_{n-1}+(2t+1)v_{n-1}$ for $n\geq 2$.

4. We only prove that $u_n$ satisfy the recurrence relation $u_n=(4t+1)(u_{n-1}+u_{n-2})-u_{n-3}$ for $n\geq 4$. For $n=4$, we find from (2.11) that $u_1=2t+1$, $u_2=8t^2+8t+1$, $u_3=32t^3+48t^2+18t+1$ and $u_4=128t^4+256t^3+160t^2+32t+1$. Hence

$$\begin{aligned}
u_4&=(4t+1)(u_3+u_2)-u_1\\
&=(4t+1)(32t^3+56t^2+26t+2)-(2t+1)\\
&=128t^4+256t^3+160t^2+32t+1.
\end{aligned}$$

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

$$u_{n-1}=(4t+1)(u_{n-2}+u_{n-3})-u_{n-4}. \tag{2.15}$$

Then applying the previous assertion, (2.14) and (2.15), we find that $u_n=(4t+1)(u_{n-1}+u_{n-2})-u_{n-3}$ for $n\geq 4$.

5. Let $t=1$. Then it is easily seen that $\sqrt{2}=[1;\overline{2}]$. Now let $t>1$. Then

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

So $\sqrt{t^2+t}=[t;\overline{2,2t}]$.

6. It is easily seen that $(u_1, v_1) = (2t+1, 2)$ is a solution since $\frac{u_1}{v_1} = [t; 2] = t + \frac{1}{2} = \frac{2t+1}{2}$. Let us assume that $(u_n, v_n)$ is a solution of $\widetilde{D}$, that is, $u_n^2 - (t^2+t)v_n^2 = 1$. Then by (2.12), we derive

$$\frac{u_{n+1}}{v_{n+1}} = t + \cfrac{1}{2 + \cfrac{1}{2t + \cfrac{1}{2 + \cfrac{1}{2t + \cfrac{1}{\cdots + 2t + \frac{1}{2}}}}}} = t + \cfrac{1}{2 + \cfrac{1}{t + t + \cfrac{1}{2 + \cfrac{1}{2t + \cfrac{1}{\cdots + 2t + \frac{1}{2}}}}}} = t + \cfrac{1}{2 + \cfrac{1}{t + \frac{u_n}{v_n}}}$$

$$= \frac{(2t+1)u_n + (2t^2+2t)v_n}{2u_n + (2t+1)v_n}. \tag{2.16}$$

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

$$u_{n+1}^2 - (t^2+t)v_{n+1}^2 = \big((2t+1)u_n + (2t^2+2t)v_n\big)^2 - (t^2+t)\big(2u_n + (2t+1)v_n\big)^2 = 1.$$

This completes the proof. □

*Example 2.1* Let $t = 5$. Then $(u_1, v_1) = (11, 2)$ is the fundamental solution of $\widetilde{D}$ : $u^2 - 30v^2 = 1$ and some other solutions are

$$(u_2, v_2) = (241, 44), \qquad (u_3, v_3) = (5291, 966), \qquad (u_3, v_3) = (5291, 966),$$
$$(u_4, v_4) = (116161, 21208), \qquad (u_5, v_5) = (2550251, 465610),$$
$$(u_6, v_6) = (55989361, 10222212).$$

Also $\sqrt{30} = [5; \overline{2, 10}]$. The solutions $(u_n, v_n)$ satisfy the relations $u_n = 21(u_{n-1} + u_{n-2}) - u_{n-3}$ and $v_n = 21(v_{n-1} + v_{n-2}) - v_{n-3}$ for $n \geq 4$. Also $u_n = 11u_{n-1} + 60v_{n-1}$ and $v_n = 2u_{n-1} + 11v_{n-1}$ for $n \geq 2$. Further

$$\frac{u_1}{v_1} = [5; 2] = \frac{11}{2},$$
$$\frac{u_2}{v_2} = [5; 2, 10, 2] = \frac{241}{44},$$
$$\frac{u_3}{v_3} = [5; 2, 10, 2, 10, 2] = \frac{5291}{966},$$
$$\frac{u_4}{v_4} = [5; 2, 10, 2, 10, 2, 10, 2] = \frac{116161}{21208},$$
$$\frac{u_5}{v_5} = [5; 2, 10, 2, 10, 2, 10, 2, 10, 2] = \frac{2550251}{465610},$$
$$\frac{u_6}{v_6} = [5; 2, 10, 2, 10, 2, 10, 2, 10, 2, 10, 2] = \frac{55989361}{10222212}.$$

From above theorem we can give the following result.

**Corollary 2.2** *The base of the transformation $T$ in (2.3) is the fundamental solution of $\widetilde{D}$, that is $T[h;k]=\{h,k\}=\{u_1,v_1\}$.*

*Proof* We proved in above theorem that $(u_1,v_1)=(2t+1,2)$ is the fundamental solution of $\widetilde{D}$. We also showed in (2.7) that $h=2t+1$ and $k=2$. So the base of $T$ is $T[h;k]=\{h,k\}=\{2t+1,2\}$ as we claimed. □

We see as above that the Diophantine equation $D: x^2-(t^2+t)y^2-(4t+2)x+(4t^2+4t)y=0$ can be transformed into the Diophantine equation $\widetilde{D}: u^2-(t^2+t)v^2=1$ via the transformation $T$ defined in (2.3). Also we show in (2.8) that $x=u+2t+1$ and $y=v+2$. Further we proved in Theorem 2.1 that the fundamental solution of $\widetilde{D}$ is $(u_1,v_1)=(2t+1,2)$ and the other solutions are $(u_n,v_n)$ which is defined in (2.11). So we can retransfer all results from $\widetilde{D}$ to $D$. Thus we can give the following main theorem.

**Theorem 2.3** *Let $D$ be the Diophantine equation in (2.1). Then*

(1) *The fundamental (minimal) solution of $D$ is $(x_1,y_1)=(4t+2,4)$.*
(2) *Define the sequence $\{(x_n,y_n)\}_{n\geq 1}=\{(u_n+2t+1,v_n+2)\}$, where $\{(u_n,v_n)\}$ defined in (2.11). Then $(x_n,y_n)$ is a solution of $D$. So it has infinitely many many integer solutions $(x_n,y_n)\in\mathbb{Z}\times\mathbb{Z}$.*
(3) *The solutions $(x_n,y_n)$ satisfy*

$$x_n=(2t+1)x_{n-1}+(2t^2+2t)y_{n-1}-8t^2-6t,$$
$$y_n=2x_{n-1}+(2t+1)y_{n-1}-8t-2$$

*for $n\geq 2$.*
(4) *The solutions $(x_n,y_n)$ satisfy the recurrence relations*

$$x_n=(4t+1)(x_{n-1}+x_{n-2})-x_{n-3}-16t^2-8t,$$
$$y_n=(4t+1)(y_{n-1}+y_{n-2})-y_{n-3}-16t$$

*for $n\geq 4$.*

*Example 2.2* Some integer solutions of $D$ are

$$\begin{aligned}
(x_1,y_1)&=(4t+2,4),\\
(x_2,y_2)&=(8t^2+10t+2,8t+6),\\
(x_3,y_3)&=(32t^3+48t^2+20t+2,32t^2+32t+8),\\
(x_4,y_4)&=(128t^4+256t^3+160t^2+34t+2,128t^3+192t^2+80t+10),\\
(x_5,y_5)&=(512t^5+1280t^4+1120t^3+400t^2+52t+2,512t^4+1024t^3+672t^2\\
&\qquad +160t+12).
\end{aligned}$$

## 3 The Diophantine equation $x^2-(t^2+t)y^2-(4t+2)x+(4t^2+4t)y=0$ over $\mathbb{F}_p$

In this section, we will consider the integer solutions of $D$ defined in (2.1) over finite fields $\mathbb{F}_p$ for primes $p\geq 5$. We show that $D$ becomes $\widetilde{D}$ which is defined in (2.10). Now let $t\in\mathbb{F}_p^*$ and let $t^2+t\equiv d(\text{mod } p)$. Then $\widetilde{D}$ becomes

$$\widetilde{D}_p^d : u^2-dv^2\equiv 1(\text{mod } p). \tag{3.1}$$

Set $\widetilde{D}_p^d(\mathbb{F}_p)=\{(u,v)\in\mathbb{F}_p\times\mathbb{F}_p : u^2-dv^2\equiv 1(\text{mod } p)\}$. Then we can give the following theorem.

**Theorem 3.1** *Let $\widetilde{D}_p^d$ be the Diophantine equation in* (3.1).

1. *If $p\equiv 1,7(\text{mod } 8)$, then*

$$\#\widetilde{D}_p^d(\mathbb{F}_p)=\begin{cases} p+1 & \textit{for } d\notin Q_p,\\ p-1 & \textit{for } d\in Q_p.\end{cases}$$

2. *If $p\equiv 3,5(\text{mod } 8)$, then*

$$\#\widetilde{D}_p^d(\mathbb{F}_p)=\begin{cases} p+1 & \textit{for } d\in Q_p,\\ p-1 & \textit{for } d\notin Q_p,\end{cases}$$

*where $Q_p$ denote the set of quadratic residues.*

*Proof* 1. Let $p\equiv 1,7(\text{mod } 8)$. Then we have two cases:

Case (1) Let $p\equiv 1(\text{mod } 8)$ and let let $d\in Q_p$. If $v=0$, then $u^2\equiv 1(\text{mod } p)$ and hence $u=1$ and $u=p-1$. So the Diophantine equation $\widetilde{D}_p^d$ has two integer solutions $(1,0)$ and $(p-1,0)$. If $u=0$, then $-dv^2\equiv 1(\text{mod } p)$ has two solutions $v_1,v_2$. So $\widetilde{D}_p^d$ has two integer solutions $(0,v_1)$ and $(0,v_2)$. Now let $S_p=\mathbb{F}_p^*-\{1,p-1\}$. Then there are $\frac{p-5}{2}$ points $u$ in $S_p$ such that $\frac{u^2-1}{d}$ is a square. Set $\frac{u^2-1}{d}=c^2$ for some $c\neq 0$. Then $v^2\equiv c^2(\text{mod}\,p)\Leftrightarrow v\equiv\pm c(\text{mod}\,p)$. So the Diophantine equation $\widetilde{D}_p^d$ 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 $2(\frac{p-5}{2})=p-5$ solutions. We see as above that it has also four solutions $(1,0),(p-1,0),(0,v_1)$ and $(0,v_2)$. Therefore $\widetilde{D}_p^d$ has $p-5+4=p-1$ integer solutions. Now let $d\notin Q_p$. If $v=0$, then $u^2\equiv 1(\text{mod } p)$ and hence $u=1$ and $u=p-1$. So the Diophantine equation $\widetilde{D}_p^d$ has two integer solutions $(1,0)$ and $(p-1,0)$. If $u=0$, then $-dv^2\equiv 1(\text{mod } p)$ has no solution. So $\widetilde{D}_p^d$ has no integer solution $(0,v)$. Let $L_p=\mathbb{F}_p^*-\{1,p-1\}$. Then there are $\frac{p-1}{2}$ points $u$ in $L_p$ such that $\frac{u^2-1}{d}$ is a square. Set $\frac{u^2-1}{d}=j^2$ for some $j\neq 0$. Then $v^2\equiv j^2(\text{mod}\,p)\Leftrightarrow v\equiv\pm j\,(\text{mod}\,p)$. So the Diophantine equation $\widetilde{D}_p^d$ has two solutions $(u,j)$ and $(u,-j)$, that is, for each $u$ in $L_p$, $\widetilde{D}_p^d$ has two solutions. So it has $2(\frac{p-1}{2})=p-1$ solutions. We see as above that it has also two solutions $(1,0)$ and $(p-1,0)$. So $\widetilde{D}_p^d$ has $p-1+2=p+1$ integer solutions.

Case (2) Let $p\equiv 7(\text{mod } 8)$ and let $d\in Q_p$. If $v=0$, then $u^2\equiv 1(\text{mod } p)$ and hence $u=1$ and $u=p-1$. So the Diophantine equation $\widetilde{D}_p^d$ has two integer solutions $(1,0)$ and $(p-1,0)$. If $u=0$, then $-dv^2\equiv 1(\text{mod } p)$ has no solution $v$. So $\widetilde{D}_p^d$ has no integer solution $(0,v)$. Now let $H_p=\mathbb{F}_p^*-\{1,p-1\}$. Then there are $\frac{p-3}{2}$ points $u$ in $H_p$ such that $\frac{u^2-1}{d}$ is a square. Set $\frac{u^2-1}{d}=k^2$ for some $k\neq 0$. Then $v^2\equiv k^2(\text{mod}\, p)\Leftrightarrow v\equiv \pm k(\text{mod}\, p)$. So the Diophantine equation $\widetilde{D}_p^d$ has two solutions $(u,k)$ and $(u,-k)$, that is, for each $u$ in $H_p$, $\widetilde{D}_p^d$ has two solutions. So it has $2(\frac{p-3}{2})=p-3$ solutions. We see as above that it has also two solutions $(1,0)$ and $(p-1,0)$. Therefore $\widetilde{D}_p^d$ has $p-3+2=p-1$ integer solutions. Let $d\notin Q_p$. If $v=0$, then $u^2\equiv 1(\text{mod } p)$ and hence $u=1$ and $u=p-1$. So the Diophantine equation $\widetilde{D}_p^d$ has two integer solutions $(1,0)$ and $(p-1,0)$. If $u=0$, then $-dv^2\equiv 1(\text{mod } p)$ has two solutions $v_1,v_2$. So $\widetilde{D}_p^d$ has two integer solutions $(0,v_1)$ and $(0,v_2)$. Now let $K_p=\mathbb{F}_p^*-\{1,p-1\}$. Then there are $\frac{p-3}{2}$ points $u$ in $K_p$ such that $\frac{u^2-1}{d}$ is a square. Set $\frac{u^2-1}{d}=m^2$ for some $m\neq 0$. Then $v^2\equiv m^2(\text{mod}\, p)\Leftrightarrow v\equiv \pm m(\text{mod}\, p)$. So the Diophantine equation $\widetilde{D}_p^d$ has two solutions $(u,k)$ and $(u,-k)$, that is, for each $u$ in $K_p$, $\widetilde{D}_p^d$ has two solutions. So it has $2(\frac{p-3}{2})=p-3$ solutions. We see as above that it has also four solutions $(1,0)$, $(p-1,0)$, $(0,v_1)$ and $(0,v_2)$. Therefore $\widetilde{D}_p^d$ has $p-3+4=p+1$ integer solutions.

2. It can be proved as in same way that the previous assertion was proved. □

*Example 3.1* Let $t=5$. Then $d=30\equiv 8(\text{mod}\,11), 4(\text{mod}\,13), 13(\text{mod}\,17), 7(\text{mod}\,23)$. So

$$\widetilde{D}_{11}^8(\mathbb{F}_{11})=\left\{\begin{array}{c}(0,2),(0,9),(1,0),(3,1),(3,10),(5,5),(5,6),(6,5),(6,6),\\(8,1),(8,10),(10,0)\end{array}\right\},$$

$$\widetilde{D}_{13}^4(\mathbb{F}_{13})=\left\{\begin{array}{c}(0,4),(0,9),(1,0),(2,2),(2,11),(6,5),(6,8),(7,5),(7,8),\\(11,2),(11,11),(12,0)\end{array}\right\},$$

$$\widetilde{D}_{17}^{13}(\mathbb{F}_{17})=\left\{\begin{array}{c}(0,8),(0,9),(1,0),(3,7),(3,10),(4,3),(4,14),(6,2),(6,15),\\(11,2),(11,15),(13,3),(13,14),(14,7),(14,10),(16,0)\end{array}\right\},$$

$$\widetilde{D}_{23}^7(\mathbb{F}_{23})=\left\{\begin{array}{c}(0,6),(0,17),(1,0),(4,9),(4,14),(8,3),(8,20),(9,8),(9,15),\\(10,1),(10,22),(11,2),(11,21),(12,2),(12,21),(13,1),\\(13,22),(14,8),(14,15),(15,3),(15,20),(19,9),(19,14),(22,0)\end{array}\right\}$$

and hence $\#\widetilde{D}_{11}^8(\mathbb{F}_{11})=12$, $\#\widetilde{D}_{131}^4(\mathbb{F}_{13})=12$, $\#\widetilde{D}_{17}^{13}(\mathbb{F}_{17})=16$ and $\#\widetilde{D}_{23}^7(\mathbb{F}_{23})=24$.

For the Diophantine equation $D$, we set

$$D(\mathbb{F}_p)=\{(x,y)\in\mathbb{F}_p\times\mathbb{F}_p : x^2-(t^2+t)y^2-(4t+2)x+(4t^2+4t)y\equiv 0(\text{mod } p)\}.$$

Then we can give the following theorem.

**Theorem 3.2** *Let D be the Diophantine equation in* (2.1).

(1) *If* $p \equiv 1, 7 (\text{mod } 8)$, *then*

$$\#D(\mathbb{F}_p) = \begin{cases} p+1 & for\ t^2+t \notin Q_p, \\ p-1 & for\ t^2+t \in Q_p. \end{cases}$$

(2) *If* $p \equiv 3, 5 (\text{mod } 8)$, *then*

$$\#D(\mathbb{F}_p) = \begin{cases} p+1 & for\ t^2+t \in Q_p, \\ p-1 & for\ t^2+t \notin Q_p. \end{cases}$$

## References

1. Arya, S.P.: On the Brahmagupta-Bhaskara equation. Math. Educ. **8**(1), 23–27 (1991)
2. Baltus, C.: Continued fractions and the Pell equations: the work of Euler and Lagrange. Comm. Anal. Theory Contin. Fractions **3**, 4–31 (1994)
3. Barbeau, E.: Pell's Equation. Springer, Berlin (2003)
4. Edwards, H.M.: Fermat's Last Theorem. A Genetic Introduction to Algebraic Number Theory. Graduate Texts in Mathematics, vol. 50. Springer, New York (1996). Corrected reprint of the 1977 original
5. Hensley, D.: Continued Fractions. World Scientific, Singapore (2006)
6. Kaplan, P., Williams, K.S.: Pell's equations $x^2 - my^2 = -1, -4$ and continued fractions. J. Number Theory **23**, 169–182 (1986)
7. Lenstra, H.W.: Solving the Pell equation. Not. AMS **49**(2), 182–192 (2002)
8. Matthews, K.: The Diophantine equation $x^2 - Dy^2 = N$, $D > 0$. Expo. Math. **18**, 323–331 (2000)
9. Mollin, R.A., Poorten, A.J., Williams, H.C.: Halfway to a solution of $x^2 - Dy^2 = -3$. J. Theor. Nr. Bordx. **6**, 421–457 (1994)
10. Mollin, R.A.: Simple continued fraction solutions for Diophantine equations. Expo. Math. **19**(1), 55–73 (2001)
11. Mollin, R.A., Cheng, K., Goddard, B.: The Diophantine equation $AX^2 - BY^2 = C$ solved via continued fractions. Acta Math. Univ. Comen. **71**(2), 121–138 (2002)
12. Mollin, R.A.: The Diophantine equation $ax^2 - by^2 = c$ and simple continued fractions. Int. Math. J. **2**(1), 1–6 (2002)
13. Mollin, R.A.: A continued fraction approach to the Diophantine equation $ax^2 - by^2 = \pm 1$. JP J. Algebra Number Theory Appl. **4**(1), 159–207 (2004)
14. Mollin, R.A.: A note on the Diophantine equation $D_1x^2 + D_2 = ak^n$. Acta Math. Acad. Paedagog. Nyireg. **21**, 21–24 (2005)
15. Mollin, R.A.: Quadratic Diophantine equations $x^2 - Dy^2 = c^n$. Ir. Math. Soc. Bull. **58**, 55–68 (2006)
16. Niven, I., Zuckerman, H.S., Montgomery, H.L.: An Introduction to the Theory of Numbers, 5th edn. Wiley, New York (1991)
17. Stevenhagen, P.: A density conjecture for the negative Pell equation. Comput. Algebra Number Theory Math. Appl. **325**, 187–200 (1992)
18. Tekcan, A.: Pell equation $x^2 - Dy^2 = 2$, II. Bull. Ir. Math. Soc. **54**, 73–89 (2004)
19. Tekcan, A., Bizim, O., Bayraktar, M.: Solving the Pell equation using the fundamental element of the field $\mathbb{Q}(\sqrt{\Delta})$. South East Asian Bull. Math. **30**, 355–366 (2006)
20. Tekcan, A.: The Pell equation $x^2 - Dy^2 = \pm 4$. Appl. Math. Sci. **1**(8), 363–369 (2007)
21. Tekcan, A., Gezer, B., Bizim, O.: On the integer solutions of the Pell equation $x^2 - dy^2 = 2^t$. Int. J. Comput. Math. Sci. **1**(3), 204–208 (2007)
22. Tekcan, A.: The Pell equation $x^2 - (k^2 - k)y^2 = 2^t$. Int. J. Comput. Math. Sci. **2**(1), 5–9 (2008)
23. Tekcan, A.: The Diophantine equation $4y^2 - 4yx - 1 = 0$, curves and conics over finite fields. Math. Rep. (accepted for publication)