THE NUMBER OF SOLUTIONS OF PELL EQUATIONS $x^2 - ky^2 = N$ AND $x^2 + xy - ky^2 = N$ OVER $\mathbb{F}_p$

AHMET TEKCAN

ABSTRACT. Let p be a prime number such that $p \equiv 1, 3 (\mathrm{mod}\, 4)$, let $\mathbb{F}_p$ be a finite field, let $N \in \mathbb{F}_p^* = \mathbb{F}_p - \{0\}$ be a fixed. Let $P_p^k(N) : x^2 - ky^2 = N$ and $\widetilde{P}_p^k(N) : x^2 + xy - ky^2 = N$ be two Pell equations over $\mathbb{F}_p$, where $k = \frac{p-1}{4}$ or $k = \frac{p-3}{4}$, respectively. Let $P_p^k(N)(\mathbb{F}_p)$ and $\widetilde{P}_p^k(N)(\mathbb{F}_p)$ denote the set of integer solutions of the Pell equations $P_p^k(N)$ and $\widetilde{P}_p^k(N)$, respectively. In the first section we give some preliminaries from general Pell equation $x^2 - ky^2 = \pm N$. In the second section, we determine the number of integer solutions of $P_p^k(N)$. We proved that $P_p^k(N)(\mathbb{F}_p) = p + 1$ if $p \equiv 1 (\mathrm{mod}\, 4)$ or $p \equiv 7 (\mathrm{mod}\, 12)$ and $P_p^k(N)(\mathbb{F}_p) = p - 1$ if $p \equiv 11 (\mathrm{mod}\, 12)$. In the third section we consider the Pell equation $\widetilde{P}_p^k(N)$. We proved that $\widetilde{P}_p^k(N)(\mathbb{F}_p) = 2p$ if $p \equiv 1 (\mathrm{mod}\, 4)$ and $N \in Q_p$; $\widetilde{P}_p^k(N)(\mathbb{F}_p) = 0$ if $p \equiv 1 (\mathrm{mod}\, 4)$ and $N \notin Q_p$; $\widetilde{P}_p^k(N)(\mathbb{F}_p) = p + 1$ if $p \equiv 3 (\mathrm{mod}\, 4)$.

AMS Subject Classification 2000: Primary, 11E15; Secondary, 11E18, 11E25.
Keywords: Pell equation, solutions of the Pell equation, finite field.
Date: 23.02.2007.

1. INTRODUCTION.

Let $k \neq 1$ be any positive non-square integer and N be any fixed integer. The equation

$$x^2 - ky^2 = \pm N \tag{1.1}$$

is known as Pell equation, and is named after John Pell (1611-1685), a mathematician who searched for integer solutions to equations of this type in the seventeenth century. Ironically, Pell was not the first to work on this problem, nor did he contribute to our knowledge for solving it. Euler (1707-1783), who brought us the ψ-function, accidentally named the equation after Pell, and the name stuck.

The Pell equation $x^2 - ky^2 = \pm 1$ is known the classical Pell equation. The equation $x^2 - ky^2 = 1$, was first studied by Brahmagupta (598-670) and Bhaskara (1114-1185). 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.

The Pell equation $x^2 - ky^2 = 1$ has infinitely many integer solutions (x_n, y_n) for $n \geq 1$. The first non-trivial positive integer solution (x_1, y_1) (in this case x_1 or $x_1 + y_1\sqrt{k}$ is minimum) 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 of $x^2 - ky^2 = 1$, then the n-th positive solution of it, say (x_n, y_n), is defined by the equality $x_n + y_n\sqrt{k} = (x_1 + y_1\sqrt{k})^n$ for integer $n \geq 2$. (Furthermore, all nontrivial solutions can be obtained considering the four cases $(\pm x_n, \pm y_n)$ for $n \geq 1$.) There are several methods for finding the fundamental solution of Pell equation $x^2 - ky^2 = 1$ for a positive non-square integer k, e.g., the cyclic method [1, p.30], known in India in the 12-th century, or the slightly less efficient but more regular English method (17-th century) which produce all solutions of $x^2 - ky^2 = 1$ [4, p.32]. But the most efficient method for finding the fundamental solution is based on the simple finite continued fraction expansion of $\sqrt{k}$ [3, p.154]. Many authors such as Kaplan and Williams [2], Lenstra [4], Matthews [5], Mollin (also Poorten and Williams) [6,7,8], Smarandache [9], Stevenhagen [10], Stroeker [11], Tekcan [12,13,14], Walsh [15] and the others consider some specific Pell equations and their integer solutions.

2. The Pell Equation $P_p^k(N) : x^2 - ky^2 = N$ Over $\mathbb{F}_p$.

Let $p \equiv 1, 3 (\mathrm{mod}\, 4)$ be a prime number, let $\mathbb{F}_p$ be a finite field, and let $N \in \mathbb{F}_p^* = \mathbb{F}_p - \{0\}$ be a fixed. Let

$$P_p^k(N) : x^2 - ky^2 = N \tag{2.1}$$

be a Pell equation over $\mathbb{F}_p$, where $k = \frac{p-1}{4}$ or $k = \frac{p-3}{4}$, respectively. In this paper we will determine the number of integer solutions of the Pell equation $P_p^k(N)$ over $\mathbb{F}_p$.

Theorem 2.1. *Let* $P_p^k(N)(\mathbb{F}_p) = \{(x, y) \in \mathbb{F}_p \times \mathbb{F}_p : x^2 - ky^2 = N\}$. *Then*

$$P_p^k(N)(\mathbb{F}_p) = \begin{cases} p+1 & \text{if } p \equiv 1 (mod 4) \text{ or } p \equiv 7 (mod 12) \\ p-1 & \text{if } p \equiv 11 (mod 12). \end{cases}$$

Proof. Let $p \equiv 1 (\mathrm{mod}\, 4)$, say $p = 1 + 4k$ for $k \in \mathbb{F}_p^*$. Let Q_p denote the set of quadratic residues in $\mathbb{F}_p$. Note that $k \in Q_p$, that is, k quadratic residue mod p. Now consider the Pell equation $P_p^k(N) : x^2 - ky^2 = N$. Then we have two cases:

Case 1: Let $N \in Q_p$, say $N = t^2$ for $t \in \mathbb{F}_p^*$. If $y = 0$, then

$$x^2 \equiv t^2 (\mathrm{mod}\, p) \Leftrightarrow x \equiv \pm t (\mathrm{mod}\, p),$$

that is, there are two integer solutions $(t, 0)$ and $(p - t, 0)$ of $P_p^k(N)$. If $x = 0$, then

$$-ky^2 \equiv t^2 (\mathrm{mod}\, p) \Leftrightarrow y^2 \equiv \pm \frac{t^2}{k} (\mathrm{mod}\, p).$$

Note that t^2/k is a square $\mathrm{mod}\, p$, since k is a quadratic residue $\mathrm{mod}\, p$. Let $m^2 = \frac{t^2}{k}$ for $m \neq 0$. Then

$$y^2 \equiv m^2 \Leftrightarrow y \equiv \pm m (\mathrm{mod}\, p),$$

that is, there are two integer solutions $(0, m)$ and $(0, p - m)$ of $P_p^k(N)$. Set $\mathbb{F}_p^{**} = \mathbb{F}_p - \{0, t, p - t\}$. Then there are $\frac{p-5}{2}$ points x in $\mathbb{F}_p^{**}$ such that $\frac{x^2 - t^2}{k}$ a square. Let $x = u$ be a point in $\mathbb{F}_p^{**}$ such that $\frac{u^2 - t^2}{k}$ a square. Set $\frac{u^2 - t^2}{k} = v^2$. Then

$$y^2 \equiv v^2 (\mathrm{mod}\, p) \Leftrightarrow y \equiv \pm v (\mathrm{mod}\, p).$$

Therefore there are two integer solutions (u, v) and $(u, p - v)$ of $P_p^k(N)$, that is, for each x in $\mathbb{F}_p^{**}$ such that $\frac{x^2 - t^2}{k}$ a square, then there are two integer solutions of $P_p^k(N)$. Hence there are $2\left(\frac{p-5}{2}\right) = p - 5$ integer solutions of $P_p^k(N)$. We see as above that there are four integer solutions $(t, 0), (p - t, 0), (0, m)$ and $(0, p - m)$ of $P_p^k(N)$. Consequently there are total $p - 5 + 4 = p - 1$ integer solutions, that is, $P_p^k(N)(\mathbb{F}_p) = p - 1$.

Case 2: Let $N \notin Q_p$. If $y = 0$, then

$$x^2 \equiv N (\mathrm{mod}\, p)$$

has no solution. If $x = 0$, then

$$-ky^2 \equiv N (\mathrm{mod}\, p)$$

has no solution since N/k is not a quadratic residue $\mathrm{mod}\, p$. Set $\mathbb{F}_p^{**} = \mathbb{F}_p - \{0\}$. Then there are $\frac{p-1}{2}$ points x in $\mathbb{F}_p^{**}$ such that $\frac{x^2 - N}{k}$ a square. Let $x = u$ be a point in $\mathbb{F}_p^{**}$ such that $\frac{u^2 - N}{k}$ a square. Set $\frac{u^2 - N}{k} = v^2$. Then

$$y^2 \equiv v^2 (\mathrm{mod}\, p) \Leftrightarrow y \equiv \pm v (\mathrm{mod}\, p).$$

Therefore there are two integer solutions (u, v) and $(u, p - v)$, that is, for each x in $\mathbb{F}_p^{**}$ such that $\frac{x^2 - N}{k}$ a square, then there are two integer solutions. Hence there are $2\left(\frac{p-1}{2}\right) = p - 1$ integer solutions of $P_p^k(N)$.

Now let $p \equiv 3 (\mathrm{mod}\, 4)$. Then we have to consider the problem either $p \equiv 1 (\mathrm{mod}\, 6)$ or $p \equiv 5 (\mathrm{mod}\, 6)$. Let $p \equiv 1 (\mathrm{mod}\, 6)$. Then by Chinese Remainder theorem $p \equiv 7 (\mathrm{mod}\, 12)$. Then we have two cases:

Case 1: Let $N \in Q_p$, say $N = t^2$ for $t \in \mathbb{F}_p^*$. If $y = 0$, then

$$x^2 \equiv t^2 (\mathrm{mod}\, p) \Leftrightarrow x \equiv \pm t (\mathrm{mod}\, p),$$

that is, there are two integer solutions $(t, 0)$ and $(p - t, 0)$ of $P_p^k(N)$. If $x = 0$, then

$$-ky^2 \equiv t^2 (\mathrm{mod}\, p) \Leftrightarrow y^2 \equiv \pm \frac{t^2}{k} (\mathrm{mod}\, p)$$

has no solution since t^2/k is not a square mod p. Set $\mathbb{F}_p^{**} = \mathbb{F}_p - \{0\}$. Then there are $\frac{p-3}{2}$ points x in $\mathbb{F}_p^{**}$ such that $\frac{x^2 - t^2}{k}$ a square. Let $x = u$ be a point in $\mathbb{F}_p^{**}$ such that $\frac{u^2 - t^2}{k}$ a square. Set $\frac{u^2 - t^2}{k} = v^2$. Then

$$y^2 \equiv v^2 (\mathrm{mod}\, p) \Leftrightarrow y \equiv \pm v (\mathrm{mod}\, p),$$

that is, there are two integer solutions (u, v) and $(u, p - v)$. Hence for each x in $\mathbb{F}_p^{**}$ such that $\frac{x^2 - t^2}{k}$ a square, then there are two integer solutions. Hence there are $2\left(\frac{p-3}{2}\right) = p - 3$ integer solutions. We see as above that there are two integer solutions $(t, 0)$ and $(p - t, 0)$. Consequently there are total $p - 3 + 2 = p - 1$ integer solutions of $P_p^k(N)$.

Case 2: Let $N \notin Q_p$. If $y = 0$, then

$$x^2 \equiv N (\mathrm{mod}\, p)$$

has no solution. If $x = 0$, then

$$-ky^2 \equiv N (\mathrm{mod}\, p) \Leftrightarrow y^2 \equiv \pm \frac{N}{k} (\mathrm{mod}\, p)$$

has two solutions since N/k is a square mod p. Let $m^2 = \frac{N}{k}$. Then

$$y^2 \equiv m^2 (\mathrm{mod}\, p) \Leftrightarrow y \equiv \pm m (\mathrm{mod}\, p),$$

that is, there are two integer solutions $(0, m)$ and $(0, p - m)$ of $P_p^k(N)$. Set $\mathbb{F}_p^{**} = \mathbb{F}_p - \{0\}$. Then there are $\frac{p-3}{2}$ points x in $\mathbb{F}_p^{**}$ such that $\frac{x^2 - N}{k}$ a square. Let $x = u$ be a point in $\mathbb{F}_p^{**}$ such that $\frac{u^2 - N}{k}$ a square. Set $\frac{u^2 - N}{k} = v^2$. Then

$$y^2 \equiv v^2 (\mathrm{mod}\, p) \Leftrightarrow y \equiv \pm v (\mathrm{mod}\, p).$$

Therefore there are two integer solutions (u, v) and $(u, p - v)$, that is, for each x in $\mathbb{F}_p^{**}$ such that $\frac{x^2 - N}{k}$ a square, then there are two integer solutions. Hence there are $2\left(\frac{p-3}{2}\right) = p - 3$ integer solutions. We see as above that there are two integer solutions $(0, m)$ and $(0, p - m)$. Consequently there are total $p - 3 + 2 = p - 1$ integer solutions of $P_p^k(N)$.

Let $p \equiv 5 (\mathrm{mod}\, 6)$. Then by Chinese Remainder theorem $p \equiv 11 (\mathrm{mod}\, 12)$. Then we have two cases:

Case 1: Let $N \in Q_p$, say $N = t^2$ for $t \in \mathbb{F}_p^*$. If $y = 0$, then

$$x^2 \equiv t^2 (\mathrm{mod}\, p) \Leftrightarrow x \equiv \pm t (\mathrm{mod}\, p),$$

that is, there are two integer solutions $(t,0)$ and $(p-t,0)$ of $P_p^k(N)$. If $x=0$, then

$$-ky^2 \equiv t^2 (\mathrm{mod}\, p) \Leftrightarrow y^2 \equiv \pm\frac{t^2}{k} (\mathrm{mod}\, p)$$

has two solutions since t^2/k a square mod p. Let $m^2 = \frac{t^2}{k}$. Then

$$y^2 \equiv m^2 (\mathrm{mod}\, p) \Leftrightarrow y \equiv \pm m (\mathrm{mod}\, p),$$

that is, there are two integer solutions $(0,m)$ and $(0,p-m)$ of $P_p^k(N)$. Set $\mathbb{F}_p^{**} = \mathbb{F}_p - \{0,t,p-t\}$. Then there are $\frac{p-3}{2}$ points x in $\mathbb{F}_p^{**}$ such that $\frac{x^2-t^2}{k}$ a square. Let $x=u$ be a point in $\mathbb{F}_p^{**}$ such that $\frac{u^2-t^2}{k}$ a square. Set $\frac{u^2-t^2}{k} = v^2$. Then

$$y^2 \equiv v^2 (\mathrm{mod}\, p) \Leftrightarrow y \equiv \pm v (\mathrm{mod}\, p).$$

Therefore there are two integer solutions (u,v) and $(u,p-v)$, that is, for each x in $\mathbb{F}_p^{**}$ such that $\frac{x^2-t^2}{k}$ a square, then there are two integer solutions. Hence there are $2\left(\frac{p-3}{2}\right) = p-3$ integer solutions. We see as above that there are four integer solutions $(t,0),(p-t,0),(0,m)$ and $(0,p-m)$. Consequently there are total $p-3+4 = p+1$ integer solutions of $P_p^k(N)$.

Case 2: Let $N \notin Q_p$. If $y=0$, then

$$x^2 \equiv N (\mathrm{mod}\, p)$$

has no solution and if $x=0$, then

$$-ky^2 \equiv N (\mathrm{mod}\, p) \Leftrightarrow y^2 \equiv \pm\frac{N}{k} (\mathrm{mod}\, p)$$

has no solution since N/k is not a square mod p. Set $\mathbb{F}_p^{**} = \mathbb{F}_p - \{0\}$. Then there are $\frac{p+1}{2}$ points x in $\mathbb{F}_p^{**}$ such that $\frac{x^2-N}{k}$ a square. Let $x=u$ be a point in $\mathbb{F}_p^{**}$ such that $\frac{u^2-N}{k}$ a square. Set $\frac{u^2-N}{k} = v^2$. Then

$$y^2 \equiv v^2 (\mathrm{mod}\, p) \Leftrightarrow y \equiv \pm v (\mathrm{mod}\, p).$$

Therefore there are two integer solutions (u,v) and $(u,p-v)$, that is, for each x in $\mathbb{F}_p^{**}$ such that $\frac{x^2-N}{k}$ a square, then there are two integer solutions. Consequently there are $2\left(\frac{p+1}{2}\right) = p+1$ integer solutions of $P_p^k(N)$. □

Example 2.1. 1. *Let* $p=17$. *Then*

$$P_{17}^4(2)(\mathbb{F}_{17}) = \left\{ \begin{array}{c} (0,2),(0,15),(1,0),(3,6),(3,11),(4,5),(4,12),(6,8),(6,9), \\ (11,8),(11,9),(13,5),(13,12),(14,6),(14,11),(16,0) \end{array} \right\}$$

and

$$P_{17}^4(3)(\mathbb{F}_{17}) = \left\{ \begin{array}{c} (1,5),(1,12),(2,8),(2,9),(4,4),(4,13),(6,2),(6,15),(11,2), \\ (11,15),(13,4),(13,13),(15,8),(15,9),(16,5),(16,12) \end{array} \right\}.$$

Note that $2 \in Q_{17}$ *and* $3 \notin Q_{17}$.

2. *Let* $p = 31$. *Then*

$$P_{31}^{7}(1)(\mathbb{F}_{31}) = \left\{ \begin{array}{c} (1,0),(3,14),(3,17),(6,6),(6,25),(8,3),(8,28),(9,10), \\ (9,21),(12,4),(12,27),(14,9),(14,22),(15,1),(15,30), \\ (16,1),(16,30),(17,9),(17,22),(19,4),(19,27),(22,10), \\ (22,21),(23,3),(23,28),(25,6),(25,25),(28,14), \\ (28,17),(30,0) \end{array} \right\}$$

and

$$P_{31}^{7}(3)(\mathbb{F}_{31}) = \left\{ \begin{array}{c} (0,2),(0,29),(2,3),(2,28),(6,7),(6,24),(9,12),(9,19), \\ (10,6),(10,25),(11,15),(11,16),(14,1),(14,30),(15,13), \\ (15,18),(16,13),(16,18),(17,1),(17,30),(20,15), \\ (20,16),(21,6),(21,25),(22,12),(22,19),(25,7), \\ (25,24),(29,3),(29,28) \end{array} \right\}.$$

Note that $1 \in Q_{31}$ *and* $3 \notin Q_{31}$.

3. *Let* $p = 47$. *Then*

$$P_{47}^{11}(1)(\mathbb{F}_{47}) = \left\{ \begin{array}{c} (0,8),(0,39),(1,0),(4,11),(4,36),(6,4),(6,43),(9,12), \\ (9,35),(10,3),(10,44),(11,13),(11,34),(16,6),(16,41), \\ (18,14),(18,33),(19,15),(19,32),(20,19),(20,28), \\ (22,22),(22,25),(23,1),(23,46),(24,1),(24,46),(25,22), \\ (25,25),(27,19),(27,28),(28,15),(28,32),(29,14),(29,33), \\ (31,6),(31,41),(36,13),(36,34),(37,3),(37,44),(38,12), \\ (38,35),(41,4),(41,43),(43,11),(43,36),(46,0) \end{array} \right\}$$

and

$$P_{47}^{11}(5)(\mathbb{F}_{47}) = \left\{ \begin{array}{c} (1,16),(1,31),(2,8),(2,39),(4,1),(4,46),(5,6),(5,41), \\ (6,15),(6,32),(7,2),(7,45),(9,20),(9,27),(11,7),(11,40), \\ (12,9),(12,38),(13,19),(13,28),(20,10),(20,37),(21,22), \\ (21,45),(26,22),(26,25),(27,10),(27,37),(34,19),(34,28), \\ (35,9),(35,38),(36,7),(36,40),(38,20),(38,27),(40,2), \\ (40,45),(41,15),(41,32),(42,6),(42,41),(43,1),(43,46), \\ (45,8),(45,39),(46,16),(46,31) \end{array} \right\}.$$

Note that $1 \in Q_{47}$ *and* $5 \notin Q_{47}$.

3. The Pell Equation $\widetilde{P}_p^k(N) : x^2 + xy - ky^2 = N$ Over $\mathbb{F}_p$.

Let $p \equiv 1, 3 (\mathrm{mod}\, 4)$ be a prime number. In this section, we determine the number of integer solutions of the Pell equation

$$\widetilde{P}_p^k(N) : x^2 + xy - ky^2 = N$$

over $\mathbb{F}_p$, where $k = \frac{p-1}{4}$ or $k = \frac{p-3}{4}$, respectively.

Theorem 3.1. *Let* $\widetilde{P}_p^k(N)(\mathbb{F}_p) = \{(x,y) \in \mathbb{F}_p \times \mathbb{F}_p : x^2 + xy - ky^2 = N\}$. *Then*

$$\widetilde{P}_p^k(N)(\mathbb{F}_p) = \begin{cases} 2p & \text{if } p \equiv 1(mod 4) \text{ and } N \in Q_p \\ 0 & \text{if } p \equiv 1(mod 4) \text{ and } N \notin Q_p \\ p+1 & \text{if } p \equiv 3(mod 4). \end{cases}$$

Proof. Let $p \equiv 1(\mathrm{mod}\, 4)$. Then we have two cases:

Case 1: Let $N \in Q_p$, say $N = t^2$ for $t \in \mathbb{F}_p^*$. If $y = 0$, then

$$x^2 \equiv t^2(\mathrm{mod}\, p) \Leftrightarrow x \equiv \pm t(\mathrm{mod}\, p),$$

that is there are two integer solutions $(t, 0)$ and $(p - t, 0)$ of $\widetilde{P}_p^k(N)$. If $x = 0$, then

$$-ky^2 \equiv t^2(\mathrm{mod}\, p) \Leftrightarrow y^2 \equiv \pm\frac{t^2}{k}(\mathrm{mod}\, p)$$

has two solutions since t^2/k is a square $\mathrm{mod}\, p$. Let $m^2 = \frac{t^2}{k}$. Then

$$y^2 \equiv m^2(\mathrm{mod}\, p) \Leftrightarrow y \equiv \pm m(\mathrm{mod}\, p),$$

that is, there are two integers solutions $(0, m)$ and $(0, p-m)$ of $\widetilde{P}_p^k(N)$. Further it is easily seen that if $x = t$, then the congruence

$$t^2 + ty - ky^2 \equiv t^2(\mathrm{mod}\, p)$$

has a solution $y = y_1$, and if $x = p - t$, then the congruence

$$(p-t)^2 + (p-t)y - ky^2 \equiv t^2(\mathrm{mod}\, p)$$

has a solution $y = y_2$. So we have six integer solutions $(0, m), (0, p - m)$, $(t, 0), (t, y_1), (p - t, 0)$ and $(p - t, y_2)$. Set $\mathbb{F}_p^{**} = \mathbb{F}_p - \{0, t, p - t\}$. Then there are $p - 3$ points x in $\mathbb{F}_p^{**}$ such that the congruence $x^2 + xy - ky^2 \equiv t^2(\mathrm{mod}\, p)$ has two solutions. Let $x = u$ be a point in $\mathbb{F}_p^{**}$ such that the congruence $u^2 + uy - ky^2 \equiv t^2(\mathrm{mod}\, p)$ has two solutions $y = y_3$ and $y = y_4$. Then there are two integer solutions (u, y_3) and (u, y_4), that is, for each point x in $\mathbb{F}_p^{**}$ such that the congruence $u^2 + uy - ky^2 \equiv t^2(\mathrm{mod}\, p)$ has two solutions, then there are two integer solutions of $\widetilde{P}_p^k(N)$. Hence there are $2(p - 3) = 2p - 6$ integer solutions. We see as above that there are six integer solutions $(0, m), (0, p - m), (t, 0), (t, y_1), (p - t, 0)$ and $(p - t, y_2)$. Consequently there are total $2(p - 3) + 6 = 2p$ integer solutions of $\widetilde{P}_p^k(N)$.

Case 2: Let $N \notin Q_p$. If $y = 0$, then

$$x^2 \equiv N(\mathrm{mod}\, p)$$

has no solution, and if $x = 0$, then

$$-ky^2 \equiv N(\mathrm{mod}\, p)$$

has no solution since N/k is not a square mod p. Set $\mathbb{F}_p^{**} = \mathbb{F}_p - \{0\}$. Then there is no point x in $\mathbb{F}_p^{**}$ such that the congruence

$$x^2 + xy - ky^2 \equiv N(\mathrm{mod}\, p)$$

has a solution y. Therefore there are no integer solutions of $\widetilde{P}_p^k(N)$.

Let $p \equiv 3(\mathrm{mod}\, 4)$. Then we consider the problem either $p \equiv 7(\mathrm{mod}\, 24)$ or $p \equiv 23(\mathrm{mod}\, 24)$. First we start with $p \equiv 7(\mathrm{mod}\, 24)$. Then we have two cases:

Case 1: Let $N \in Q_p$, say $N = t^2$ for $t \in \mathbb{F}_p^*$. If $y = 0$, then

$$x^2 \equiv t^2(\mathrm{mod}\, p) \Leftrightarrow x \equiv \pm t(\mathrm{mod}\, p),$$

that is, there are two integer solutions $(t, 0)$ and $(p - t, 0)$ of $\widetilde{P}_p^k(N)$ and if $x = 0$, then

$$-ky^2 \equiv t^2(\mathrm{mod}\, p) \Leftrightarrow y^2 \equiv \pm\frac{t^2}{k}(\mathrm{mod}\, p)$$

has no solution since t^2/k is not a square mod p. Further it can be shown that if $x = t$, then the congruence

$$t^2 + ty - ky^2 \equiv t^2(\mathrm{mod}\, p)$$

has a solution $y = y_1$, and if $x = p - t$, then the congruence

$$(p-t)^2 + (p-t)y - ky^2 \equiv t^2(\mathrm{mod}\, p)$$

has a solution $y = y_2$. Therefore there are four integer solutions $(t, 0), (t, y_1), (p - t, 0)$ and $(p - t, y_2)$ of $\widetilde{P}_p^k(N)$. Set $\mathbb{F}_p^{**} = \mathbb{F}_p - \{0, t, p - t\}$. Then there are $\frac{p-3}{2}$ points x in $\mathbb{F}_p^{**}$ such that the congruence $x^2 + xy - ky^2 \equiv t^2(\mathrm{mod}\, p)$ has two solutions. Let $x = u$ be a point in $\mathbb{F}_p^{**}$ such that $u^2 + uy - ky^2 \equiv t^2(\mathrm{mod}\, p)$ has two solutions y_3, y_4. Then there are two integer solutions (u, y_3) and (u, y_4) of $\widetilde{P}_p^k(N)$, that is, for each x in $\mathbb{F}_p^{**}$ such that $x^2 + xy - ky^2 \equiv t^2(\mathrm{mod}\, p)$ has two solutions then there are two integer solutions. Hence there are $2\left(\frac{p-3}{2}\right) = p - 3$ integer solutions. We see as above that there are four integer solutions $(t, 0), (t, y_1), (p-t, 0)$ and $(p-t, y_2)$. Consequently there are total $p-3+4 = p+1$ integer solutions of $\widetilde{P}_p^k(N)$.

Case 2: Let $N \notin Q_p$. If $y = 0$, then

$$x^2 \equiv N(\mathrm{mod}\, p)$$

has no solution, and if $x = 0$, then

$$-ky^2 \equiv N(\mathrm{mod}\, p) \Leftrightarrow y^2 \equiv \pm\frac{N}{k}(\mathrm{mod}\, p)$$

has two solutions since N/k is a square mod p. Let $m^2 = \frac{N}{k}$. Then

$$y^2 \equiv m^2(\mathrm{mod}\, p) \Leftrightarrow y \equiv \pm m(\mathrm{mod}\, p),$$

that is, there are two integer solutions $(0,m)$ and $(0,p-m)$ of $\widetilde{P}_p^k(N)$. Further there exists a point $x=x_1$ in $\mathbb{F}_p^*$ such that the congruence

$$x_1^2+x_1y-ky^2\equiv N(\mathrm{mod}\,p)$$

has one solution $y=y_1$, that is (x_1,y_1) is an integer solution of $\widetilde{P}_p^k(N)$. Also $(p-x_1,p-y_1)$ is an integer solution. Set $\mathbb{F}_p^{**}=\mathbb{F}_p-\{0,x_1,p-x_1\}$. Then there are $\frac{p-3}{2}$ points x in $\mathbb{F}_p^{**}$ such that the congruence $x^2+xy-ky^2\equiv N(\mathrm{mod}\,p)$ has two solutions. Let $x=u$ be a point in $\mathbb{F}_p^{**}$ such that $u^2+uy-ky^2\equiv N(\mathrm{mod}\,p)$ has two solutions $y=y_2,y_3$. Then there are two integer solutions (u,y_2) and (u,y_3). Hence for each x, there are two integer solutions. Therefore there are $2\left(\frac{p-3}{2}\right)=p-3$ integer solutions. Note that there are four integer solutions $(0,m),(0,p-m),(x_1,y_1)$ and $(p-x_1,p-y_1)$. Consequently there are total $p-3+4=p+1$ integer solutions of $\widetilde{P}_p^k(N)$.

Finally let $p\equiv 23(\mathrm{mod}\,24)$. Then we have two cases:

Case 1: Let $N\in Q_p$, say $N=t^2$ for $t\in\mathbb{F}_p^*$. If $y=0$, then

$$x^2\equiv t^2(\mathrm{mod}\,p)\Leftrightarrow x\equiv\pm t(\mathrm{mod}\,p),$$

that is, there are two integer solutions $(t,0)$ and $(p-t,0)$ of $\widetilde{P}_p^k(N)$. Further it is easily seen that if $x=t$, then the congruence

$$t^2+ty-ky^2\equiv t^2(\mathrm{mod}\,p)$$

has one solution $y=y_1$, and if $x=p-t$, then the congruence

$$(p-t)^2+(p-t)y-ky^2\equiv t^2(\mathrm{mod}\,p)$$

has one solution $y=y_2$. If $x=0$, then

$$-ky^2\equiv t^2(\mathrm{mod}\,p)\Leftrightarrow y^2\equiv\mp\frac{t^2}{k}(\mathrm{mod}\,p)$$

has two solutions since t^2/k a square mod p. Let $m^2=\frac{t^2}{k}$. Then

$$y^2\equiv m^2(\mathrm{mod}\,p)\Leftrightarrow y\equiv\pm m(\mathrm{mod}\,p),$$

that is, there are two integer solutions $(0,m)$ and $(0,p-m)$ of $P_p^k(N)$. Further there exists a point $x=x_1$ in $\mathbb{F}_p^*$ such that the congruence

$$x_1^2+x_1y-ky^2\equiv N(\mathrm{mod}\,p)$$

has one solution $y=y_3$, that is, (x_1,y_3) is an integer solution. Also $(p-x_1,p-y_3)$ is an integer solution. Set $\mathbb{F}_p^{**}=\mathbb{F}_p-\{0,t,p-t,x_1,p-x_1\}$. Then there are $\frac{p-7}{2}$ points x in $\mathbb{F}_p^{**}$ such that the congruence $x^2+xy-ky^2\equiv t^2(\mathrm{mod}\,p)$ has two solutions. Let $x=u$ be a point such that $u^2+uy-ky^2\equiv t^2(\mathrm{mod}\,p)$ has two solutions y_4 and y_5. Then there are two integer solutions (u,y_4) and (u,y_5), that is, for each x there are two integer solutions. Hence there are $2\left(\frac{p-7}{2}\right)=$

$p-7$ integer solutions. We see as above that there are eight integer solutions $(t,0),(p-t,0),(t,y_1),(p-t,y_2),(0,m),(0,p-m),(x_1,y_3)$ and $(p-x_1,p-y_3)$. Consequently there are total $p-7+8=p+1$ integer solutions of $\widetilde{P}_p^k(N)$.

Case 2: Let $N \notin Q_p$. If $y=0$, then

$$x^2 \equiv N(\mathrm{mod}\, p)$$

has no solution, and if $x=0$, then

$$-ky^2 \equiv N(\mathrm{mod}\, p) \Leftrightarrow y^2 \equiv \pm\frac{N}{k}(\mathrm{mod}\, p)$$

has no solution since N/k is not a square mod p. Set $\mathbb{F}_p^{**}=\mathbb{F}_p-\{0\}$. Then there are $\frac{p+1}{2}$ points x in $\mathbb{F}_p^{**}$ such that the congruence $x^2+xy-ky^2 \equiv N(\mathrm{mod}\, p)$ has two solutions. Let $x=u$ be a point such that $u^2+uy-ky^2 \equiv N(\mathrm{mod}\, p)$ has two solutions y_1, y_2. Then there are two integer solutions (x,y_1) and (x,y_2), that is, for each x there are two integer solutions. Therefore there are $2\left(\frac{p+1}{2}\right)=p+1$ integer solutions of $\widetilde{P}_p^k(N)$. □

Example 3.1. 1. *Let* $p=13$. *Then*

$$\widetilde{P}_{13}^3(1)(\mathbb{F}_{13}) = \left\{ \begin{array}{c} (0,2),(0,11),(1,0),(1,9),(2,7),(2,11),(3,5),(3,9),(4,3), \\ (4,7),(5,1),(5,5),(6,3),(6,12),(7,1),(7,10),(8,8),(8,12), \\ (9,6),(9,10),(10,4),(10,8),(11,2),(11,6),(12,0),(12,4) \end{array} \right\}$$

and $\widetilde{P}_{13}^3(2)(\mathbb{F}_{13})=\{\}$. *Note that* $1 \in Q_{13}$ *and* $2 \notin Q_{13}$.

2. *Let* $p=31$. *Then*

$$\widetilde{P}_{31}^7(1)(\mathbb{F}_{31}) = \left\{ \begin{array}{c} (1,0),(1,9),(3,11),(3,16),(4,13),(4,23),(10,6),(10,22), \\ (11,1),(11,5),(12,16),(12,30),(14,13),(14,20),(15,5), \\ (15,6),(16,25),(16,26),(17,11),(17,18),(19,1),(19,15), \\ (20,26),(20,30),(21,9),(21,25),(27,8),(27,18),(18,15), \\ (28,20),(30,0),(30,22) \end{array} \right\}$$

and

$$\widetilde{P}_{31}^7(3)(\mathbb{F}_{31}) = \left\{ \begin{array}{c} (0,2),(0,29),(1,3),(1,6),(2,20),(2,29),(4,8),(4,28), \\ (7,7),(7,25),(8,1),(8,9),(9,20),(9,30),(12,23),(14,9), \\ (14,24),(17,7),(17,22),(19,8),(22,1),(22,11),(23,22), \\ (23,30),(24,6),(24,24),(27,3),(27,23),(29,2), \\ (29,11),(30,25),(30,28) \end{array} \right\}.$$

Note that $1 \in Q_{31}$ *and* $3 \notin Q_{31}$.

3. *Let* $p = 47$. *Then*

$$\widetilde{P}_{47}^{11}(1)(\mathbb{F}_{47}) = \left\{ \begin{array}{c} (0,3),(0,39),(1,0),(1,30),(2,18),(2,42),(3,1), \\ (3,42),(4,27),(4,36),(5,28),(6,15),(6,24), \\ (8,13),(8,39),(14,16),(14,28),(16,27),(16,30), \\ (17,16),(17,24),(20,7),(20,29),(21,32),(21,34), \\ (26,13),(26,15),(27,8),(27,40),(30,23),(30,31), \\ (31,17),(31,20),(33,19),(33,31),(39,8),(39,34), \\ (41,23),(41,32),(42,19),(43,1),(43,20),(44,5), \\ (44,46),(45,5),(45,29),(46,0),(46,17) \end{array} \right\}$$

and

$$\widetilde{P}_{47}^{11}(10)(\mathbb{F}_{47}) = \left\{ \begin{array}{c} (1,8),(1,22),(3,14),(3,29),(5,4),(5,5),(9,39), \\ (9,43),(10,23),(10,42),(12,10),(12,21),(13,2), \\ (13,12),(14,21),(14,23),(15,29),(15,45),(17,7), \\ (17,33),(22,12),(22,37),(23,7),(23,25),(24,22), \\ (24,40),(25,10),(25,35),(30,14),(30,40),(32,2), \\ (32,18),(33,24),(33,26),(34,35),(34,45),(35,26), \\ (35,37),(37,5),(37,24),(38,4),(38,8),(42,42), \\ (42,43),(44,18),(44,33),(46,25),(46,39) \end{array} \right\}.$$

Note that $1 \in Q_{47}$ *and* $10 \notin Q_{47}$.

References

[1] H.M. Edward. *Fermat's Last Theorem: A Genetic Introduction to Algebraic Number Theory.* Graduate Texts in Mathematics, Vol: 50, Springer-Verlag, 1977.

[2] P. Kaplan and K.S. Williams. *Pell's Equations* $x^2 - my^2 = -1, -4$ *and Continued Fractions.* Jour. Number Theory **23**(1986), 169–182.

[3] N.Koblitz. *A Course in Number Theory and Cryptography.* Graduate Texts in Mathematics, Second Edition, Springer, 1994.

[4] H.W. Lenstra. *Solving the Pell Equation.* Notices of the AMS **49**(2)(2002), 182–192.

[5] K. Matthews. *The Diophantine Equation* $x^2 - Dy^2 = N$, $D > 0$. Expositiones Math. **18**(2000), 323–331.

[6] R.A. Mollin, A.J. Poorten and H.C. Williams. *Halfway to a Solution of* $x^2 - Dy^2 = -3$. Journal de Theorie des Nombres Bordeaux, **6**(1994), 421–457.

[7] R.A. Mollin. *Polynomial Solutions for Pell's Equation Revisited.* Indian Journal of Pure and Applied Math. **28**(1997), 429–438.

[8] R.A. Mollin. *Polynomials of Pellian Type and Continued Fractions.* Serdica Math. J. Bulgarian Academy of Science, **27**(2001), 317–342.

[9] F. Smarandache. *Method to Solve the Diophantine Equation* $ax^2 - by^2 + c = 0$. In Collected Papers, Vol. 1. Lupton, AZ: Erhus University Press, 1996.

[10] P. Stevenhagen. *A Density Conjecture for the Negative Pell Equation.* Computational Algebra and Number Theory, Math. Appl. **325**(1992), 187–200.

[11] R.J. Stroeker. *How to Solve a Diophantine Equation.* Amer. Math. Monthly, **91**(1984), 385–392.

[12] A. Tekcan. *Pell Equation* $x^2 - Dy^2 = 2$ *II.* Bull. of the Irish Math. Soc.,54(2004), 73–89.
[13] A. Tekcan, O. Bizim and M. Bayraktar. *Solving the Pell Equation Using the Fundamental Element of the Field* $\mathbb{Q}(\sqrt{\Delta})$. South East Asian Bull. of Maths., 30(2006), 355–366.
[14] A. Tekcan. *The Pell Equation* $x^2 - Dy^2 = \pm 4$. App. Math. Sci., 1(8)(2007), 363–369.
[15] P.G. Walsh. *A Note on Ljunggren's Theorem About the Diophantine Equation* $aX^2 - bY^4 = 1$. Comptes Rendues Mathematical Reports of the Royal Society of Canada, 20(1998), 113–119.

ULUDAG UNIVERSITY, FACULTY OF SCIENCE, DEPARTMENT OF MATHEMATICS, GÖRÜKLE 16059. BURSA-TURKEY

E-mail address: tekcan@uludag.edu.tr

URL: http://matematik.uludag.edu.tr/AhmetTekcan.htm