World Academy of Science, Engineering and Technology
International Journal of Mathematical and Computational Sciences
Vol:3, No:11, 2009

The Diophantine Equation $y^2 - 2yx - 3 = 0$ and Corresponding Curves over $\mathbf{F}_p$

Ahmet Tekcan, Arzu Özkoç and Hatice Alkan

***Abstract*—**In this work, we consider the number of integer solutions of Diophantine equation $D : y^2 - 2yx - 3 = 0$ over $\mathbf{Z}$ and also over finite fields $\mathbf{F}_p$ for primes $p \geq 5$. Later we determine the number of rational points on curves $E_p : y^2 = P_p(x) = y_1^p + y_2^p$ over $\mathbf{F}_p$, where y_1 and y_2 are the roots of D. Also we give a formula for the sum of $x-$ and $y-$coordinates of all rational points (x, y) on E_p over $\mathbf{F}_p$.

***Keywords*—**Diophantine equation, Pell equation, quadratic form.

I. 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 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 (further to the theory of binary quadratic forms $f(x, y) = ax^2+bxy+cy^2$ see [2], [3], [5]) 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

$$ax^2 + bxy + cy^2 + dx + ey + f = 0. \quad (1)$$

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 $x^2 - dy^2 = 1$ (or in general case $x^2 - dy^2 = N$) is known the Pell equation (see [1], [4], [6], [7], [8], [9], [10], [11], [13]) 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.

Ahmet Tekcan, Arzu Özkoç and Hatice Alkan are with the Uludag University, Department of Mathematics, Faculty of Science, Bursa-TURKEY, emails: tekcan@uludag.edu.tr, aozkoc@uludag.edu.tr, halkan@uludag.edu.tr, http://matematik.uludag.edu.tr/AhmetTekcan.htm.

II. The Diophantine Equation $y^2 - 2yx - 3 = 0$.

In [7], [8], [9], [10], [11], [13], we considered some specific Pell equations and their integer solutions. In the present paper, we will consider the integer solutions of Diophantine equation

$$D : y^2 - 2yx - 3 = 0 \quad (2)$$

over $\mathbf{Z}$ and over finite fields $\mathbf{F}_p$ for primes $p \geq 5$. Now one can wonder why we consider this Diophantine equation among thousands of such Diophantine equations. Let us explain: We consider this equation since in later section we use the roots of this equation according to y, that is, $y_{1,2} = x \pm \sqrt{x^2 + 3}$, and hence we consider the curves $E_p : y^2 = P_p(x) = y_1^p + y_2^p$ over $\mathbf{F}_p$. First, we consider the integer solutions of D over $\mathbf{Z}$.

Theorem 2.1: The Diophantine equation D in (2) has four integer solutions (x, y) in $\mathbf{Z} \times \mathbf{Z}$.

Proof: For the Diophantine equation in (2), we get

$$y^2 - 2yx - 3 = 0 \Leftrightarrow y(y - 2x) = 3.$$

Hence we have the following possibilities:

y	$y - 2x$
1	3
3	1
-1	-3
-3	$-1.$

So we get four integer solutions $(x, y) = \pm(1, 3)$ and $\pm(1, -1)$ of D. ■

Now we consider the integer solutions of D over finite fields $\mathbf{F}_p$ for primes $p \geq 5$. If we consider D over $\mathbf{F}_p$, then (2) becomes

$$D_p : y^2 - 2yx - 3 \equiv 0(mod\ p). \quad (3)$$

Let $D_p(\mathbf{F}_p)$ denote the set of integer solutions (x, y) of D_p over $\mathbf{F}_p$, that is,

$$D_p(\mathbf{F}_p) = \{(x, y) \in \mathbf{F}_p \times \mathbf{F}_p : y^2 - 2yx - 3 \equiv 0(mod\ p)\}. \quad (4)$$

Then we can give the following theorem.

Theorem 2.2: Let D_p be the Diophantine equation in (3). Then

$$\#D_p(\mathbf{F}_p) = p - 1$$

for every prime $p \geq 5$.

Proof: Let $(\frac{x}{p})$ denote the Legendre symbol. We proved in [12] that

$$\left(\frac{-3}{p}\right) = \begin{cases} 1 & if\ p \equiv 1,7(mod\ 12) \\ -1 & if\ p \equiv 5,11(mod\ 12). \end{cases} \quad (5)$$

Similarly it can be shown that

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & if\ p \equiv 1,11(mod\ 12) \\ -1 & if\ p \equiv 5,7(mod\ 12). \end{cases} \quad (6)$$

Now let $x \in \mathbf{F}_p$ be given. We want to solve D_p to y. The discriminant of (3) is

$$\Delta \equiv (-2x)^2 - 4(-3) \equiv 4(x^2+3)\ (mod\ p)$$

and hence the solutions are

$$y_{1,2} \equiv \frac{2x \pm \sqrt{\Delta}}{2} \equiv x \pm \sqrt{x^2+3}\ (mod\ p). \quad (7)$$

Then we have two cases:

Case 1) Let $p \equiv 1,7(mod\ 12)$. Then by (5) we get $(\frac{-3}{p}) = 1$, that is,

$$x^2 \equiv -3(mod\ p) \Leftrightarrow x^2+3 \equiv 0\ (mod\ p) \quad (8)$$

has two solutions x_1 and x_2. So for these values of x_1 and x_2, we have two values of y_1 and y_2 from (7). Therefore there are two integer solutions (x_1, y_1) and (x_2, y_2) of D_p.

i) Let $p \equiv 1(mod\ 12)$. If $x = 0$, then the quadratic congruence $y^2 - 3 \equiv 0(mod\ p)$ has two solutions y_3 and y_4 since $(\frac{3}{p}) = 1$ by (6). So the Diophantine equation D_p has two integer solutions $(0, y_3)$ and $(0, y_4)$. Now let $H_p = \mathbf{F}_p - \{0, x_1, x_2\}$. Note that $\#H_p = p-3$. Now we consider the quadratic congruence $x^2+3 \equiv t^2(mod\ p)$. Then it is easily seen that there are $\frac{p-5}{2}$ integers $x \in H_p$ such that the congruence $x^2+3 \equiv t^2(mod\ p)$ has a solution. So from (7), we have $y_{1,2} \equiv x \pm t\ (mod\ p)$, that is, there are two solutions y_5 and y_6, that is, for each element x in H_p, there are two solutions. We say as above that there are $\frac{p-5}{2}$ elements x in H_p such that the congruence $y_{1,2} \equiv x \pm t\ (mod\ p)$ has a solution. So there are $2(\frac{p-5}{2}) = p-5$ integer solutions of (3). We know that there are four solutions $(x_1, y_1), (x_2, y_2), (0, y_3)$ and $(0, y_4)$ of (3). So there are total $p-5+4 = p-1$ integer solutions of D_p.

ii) Let $p \equiv 7(mod\ 12)$. If $x = 0$, then the quadratic congruence $y^2 - 3 \equiv 0(mod\ p)$ has no solutions since $(\frac{3}{p}) = -1$ by (6). So the Diophantine equation D_p has no integer solutions $(0, y)$. Let $G_p = \mathbf{F}_p - \{x_1, x_2\}$. Note that $\#G_p = p-2$. Then it is easily seen that the there are $\frac{p-3}{2}$ elements x in G_p such that the quadratic congruence $x^2+3 \equiv t^2(mod\ p)$ has a solution x. So we have $y_{1,2} \equiv x \pm t\ (mod\ p)$, that is, there are two solutions y_3 and y_4, that is, for each element x in G_p, there are two solutions. We know that there are $\frac{p-3}{2}$ elements x in G_p such that the congruence $x^2+3 \equiv t^2(mod\ p)$ has a solution. So there are $2(\frac{p-3}{2}) = p-3$ integer solutions. We said as above that there are also two integer solutions (x_1, y_1) and (x_2, y_2) of D_p. So there are total $p-3+2 = p-1$ integer solutions of D_p.

Case 2) Let $p \equiv 5,11(mod\ 12)$. Then by (5) we get $(\frac{-3}{p}) = -1$, that is, $x^2 \equiv -3(mod\ p)$ has no solution x. Hence the quadratic congruence

$$x^2 \equiv -3(mod\ p) \Leftrightarrow x^2+3 \equiv 0\ (mod\ p) \quad (9)$$

has no solution x. So there exist no integer $x \in \mathbf{F}_p$ such that $x^2+3 \equiv 0(mod\ p)$ has a solution.

i) Let $p \equiv 5(mod\ 12)$. If $x = 0$, then the quadratic congruence $y^2 - 3 \equiv 0(mod\ p)$ has no solutions y since $(\frac{3}{p}) = -1$ by (6). So the Diophantine equation D_p has no integer solutions $(0, y)$. Let $S_p = \mathbf{F}_p - \{0\}$. Then there are $\frac{p-1}{2}$ integers x in S_p such that the quadratic congruence $x^2+3 \equiv t^2(mod\ p)$ has a solution x. So we have $y_{1,2} \equiv x \pm t\ (mod\ p)$, that is, there are two solutions y_1 and y_2, that is, for each element x in S_p, there are two solutions. Therefore there are $2(\frac{p-1}{2}) = p-1$ integer solutions of D_p.

ii) Let $p \equiv 11(mod\ 12)$. If $x = 0$, then the quadratic congruence $y^2 - 3 \equiv 0(mod\ p)$ has two solutions y_1 and y_2 since $(\frac{3}{p}) = 1$. So the Diophantine equation D_p has two integer solutions $(0, y_1)$ and $(0, y_2)$. Now let $L_p = \mathbf{F}_p - \{0\}$. Then there are $\frac{p-3}{2}$ elements x in L_p such that the quadratic congruence $x^2+3 \equiv t^2(mod\ p)$ has a solution. So we have $y_{1,2} \equiv x \pm t\ (mod\ p)$, that is, there are two solutions y_3 and y_4, that is, for each element x in L_p, there are two solutions. So there are $2(\frac{p-3}{2}) = p-3$ integer solutions of D_p. We know that there are two integer solutions $(0, y_1)$ and $(0, y_2)$. Therefore there are total $p-3+2 = p-1$ integer solutions of D_p. ■

Example 2.1: For $p = 13, 19, 17$ and 23, the set of integer solutions of D_p over $\mathbf{F}_p$ is

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

$$D_{19}(\mathbf{F}_{19}) = \left\{ \begin{array}{c} (1,3), (1,18), (2,10), (2,13), (\mathbf{4},\mathbf{4}), \\ (5,2), (5,8), (6,5), (6,7), (13,12), \\ (13,14), (14,11), (14,17), (\mathbf{15},\mathbf{15}), \\ (17,6), (17,9), (18,1), (18,16) \end{array} \right\}$$

$$D_{17}(\mathbf{F}_{17}) = \left\{ \begin{array}{c} (1,3), (1,16), (4,10), (4,15), (7,6), \\ (7,8), (8,4), (8,12), (9,5), (9,13), \\ (10,9), (10,11), (13,2), (13,7), \\ (16,1), (16,14) \end{array} \right\}$$

$$D_{23}(\mathbf{F}_{23}) = \left\{ \begin{array}{c} (\mathbf{0},\mathbf{7}), (\mathbf{0},\mathbf{16}), (1,3), (1,22), (3,12), \\ (3,17), (6,2), (6,10), (7,18), (7,19), \\ (11,8), (11,14), (12,9), (12,15), \\ (16,4), (16,5), (17,13), (17,21), \\ (20,6), (20,11), (22,1), (22,20). \end{array} \right\}.$$

III. The Number of Rational Points on Curves over $\mathbf{F}_p$.

In this section, we consider the number of rational points on curves related to D_p. Recall that the integer solutions of D_p are $y_1 = x + \sqrt{x^2+3}$ and $y_2 = x - \sqrt{x^2+3}$. Define

$$P_n(x) = y_1^n + y_2^n \quad (10)$$

for a positive integer n. Then we can give the following theorem.

Theorem 3.1: $P_n(x) \in \mathbf{Z}[x]$ for every positive integer n.

Proof: Let n be even. Then by binomial formula we have

$$\begin{aligned}
& P_n(x) \\
= \; & y_1^n + y_2^n \\
= \; & (x+\sqrt{x^2+3})^n + (x+\sqrt{x^2+3})^n \\
= \; & \sum_{k=0}^{n} (\frac{n}{k})(x)^{n-k}(\sqrt{x^2+3})^k \\
& + \sum_{k=0}^{n} (\frac{n}{k})(x)^{n-k}(-\sqrt{x^2+1})^k \\
= \; & \left[\begin{array}{c} (\frac{n}{0})x^n + (\frac{n}{1})x^{n-1}(\sqrt{x^2+3})^1 \\ +(\frac{n}{2})x^{n-2}(\sqrt{x^2+3})^2 + \cdots \\ +(\frac{n}{n-1})x^1(\sqrt{x^2+3})^{n-1} \\ +(\frac{n}{n})(\sqrt{x^2+3})^n \end{array} \right] \\
& - \left[\begin{array}{c} (\frac{n}{0})x^n - (\frac{n}{1})x^{n-1}(\sqrt{x^2+3})^1 \\ +(\frac{n}{2})x^{n-2}(\sqrt{x^2+3})^2 + \cdots \\ -(\frac{n}{n-1})x^1(\sqrt{x^2+3})^{n-1} \\ +(\frac{n}{n})(\sqrt{x^2+3})^n \end{array} \right] \\
= \; & 2 \left[\begin{array}{c} (\frac{n}{0})x^n + (\frac{n}{2})x^{n-2}(\sqrt{x^2+3})^2 \\ + \cdots + (\frac{n}{n})(\sqrt{x^2+3})^n \end{array} \right] \\
= \; & 2\sum_{i=0}^{\frac{n}{2}} (\frac{n}{2i})x^{n-2i}(\sqrt{x^2+3})^{2i} \\
= \; & 2\sum_{i=0}^{\frac{n}{2}} (\frac{n}{2i})x^{n-2i}(x^2+3)^i.
\end{aligned}$$

Similarly it can be shown that if n is odd, then

$$P_n(x) = 2\sum_{i=0}^{\frac{n-1}{2}} (\frac{n}{2i})x^{n-2i}(x^2+3)^i.$$

Therefore $P_n(x) \in \mathbf{Z}[x]$. ■

From above theorem we can give the following result.

Corollary 3.2: $P_n(x)$ is a polynomial with integer coefficients of degree n with leading coefficients 2^n and has $\lfloor \frac{n}{2} \rfloor$ terms for every $n \geq 1$.

Now we can consider the number of rational points on curves

$$E_p : y^2 = P_p(x) \tag{11}$$

over $\mathbf{F}_p$ for primes $p \geq 5$. Let

$$E_p(\mathbf{F}_p) = \{(x,y) \in \mathbf{F}_p \times \mathbf{F}_p : y^2 = P_p(x)\}.$$

Then we have the following theorem.

Theorem 3.3: Let E_p be the curve in (11). Then

$$\#E_p(\mathbf{F}_p) = p$$

for every prime $p \geq 5$.

Proof: Recall that by Fermat's little theorem $a^{p-1} \equiv 1 \; (mod\ p)$. Also it is known that

$$\left(\frac{2}{p}\right) = \left\{ \begin{array}{ll} 1 & if\ p \equiv 1,7 (mod\, 8) \\ -1 & if\ p \equiv 3,5 (mod\, 8). \end{array} \right. \tag{12}$$

Applying Theorem 3.1, it is clear that

$$P_p(x) = c_2x^p + c_4x^{p-2} + c_6x^{p-4} + \cdots + c_{p-1}x^3 + c_{p+1}x.$$

Recall that $c_2 = 2^p$ by Corollary 3.2 and also p is a divisor of $c_4, c_6, \cdots, c_{p-1}$ and c_{p+1}. So $c_4, c_6, \cdots, c_{p-1}, c_{p+1} \equiv 0 \; (mod\ p)$ and also $c_2 = 2^p \equiv 2 (mod\ p)$ by Fermat's little theorem. So (11) becomes $E_p : y^2 = P_p(x) \equiv 2x^p (mod\ p)$. Again by Fermat's little theorem we get $x^p \equiv x (mod\ p)$. So we have

$$E_p : y^2 = P_p(x) \equiv 2x (mod\ p).$$

Then we have two cases:

Case 1) Let $p \equiv 1,7 (mod\, 8)$. Then by (12), we have $(\frac{2}{p}) = 1$.

i) Let $x \in \mathbf{F}_p^*$ be a quadratic residue, that is $(\frac{x}{p}) = 1$. Then $(\frac{2x}{p}) = (\frac{2}{p})(\frac{x}{p}) = 1.1 = 1$. So $2x$ is a quadratic residue, that is, $2x \in Q_p$. Let $2x = t^2$ for some $t \in \mathbf{F}_p^*$. Then $y^2 \equiv 2x (mod\ p) \Leftrightarrow y^2 \equiv t^2 (mod\ p) \Leftrightarrow y \equiv \pm t (mod\ p)$, that is, the quadratic congruence $y^2 \equiv 2x (mod\ p)$ has two solutions $y = t$ and $y = p - t$. So for every $x \in Q_p$, there are two rational points on E_p. Recall that $\#Q_p = \frac{p-1}{2}$. So there are $2(\frac{p-1}{2}) = p-1$ rational points on E_p. The point $(0,0)$ is also on E_p. Therefore $\#E_p(\mathbf{F}_p) = p$.

ii) Let $(\frac{x}{p}) = -1$. Then $(\frac{2x}{p}) = -1$. So $2x$ is not a quadratic residue, that is, $2x \notin Q_p$. So quadratic congruence $y^2 \equiv 2x (\text{mod}\ p)$ has no integer solutions. Therefore there is no rational point on E_p.

Case 2) Let $p \equiv 3,5 (mod\, 8)$. Then by (12), we have $(\frac{2}{p}) = -1$.

i) Let $(\frac{x}{p}) = 1$. Then $(\frac{2x}{p}) = -1$. So $2x$ is not a quadratic residue, that is, $2x \notin Q_p$. Therefore the quadratic congruence $y^2 \equiv 2x (mod\ p)$ has no integer solutions and hence there is no rational point on E_p.

ii) Let $(\frac{x}{p}) = -1$. Then $(\frac{2x}{p}) = 1$. So $2x \in Q_p$. Then as in i) of Case 1), we have total p rational points on E_p. ■

Example 3.1: For $p = 17$ and $p = 19$, the set of rational points on E_p over $\mathbf{F}_p$ is

$$\begin{aligned}
E_{17}(\mathbf{F}_{17}) &= \left\{ \begin{array}{c} (0,0),(1,\pm 6),(2,\pm 2),(4,\pm 5),(8,\pm 4), \\ (9,\pm 1),(13,\pm 3),(15,\pm 8),(16,\pm 7) \end{array} \right\} \\
E_{19}(\mathbf{F}_{19}) &= \left\{ \begin{array}{c} (0,0),(2,\pm 2),(3,\pm 5),(8,\pm 4),(10,\pm 1), \\ (12,\pm 9),(13,\pm 8),(14,\pm 3),(15,\pm 7), \\ (18,\pm 6) \end{array} \right\}.
\end{aligned}$$

Now we consider the sum of $x-$ and $y-$coordinates of all rational points (x,y) on E_p. For this reason, set

$$E_p^x(\mathbf{F}_p) = \{x \in \mathbf{F}_p : (x,y) \in E_p(\mathbf{F}_p)\}$$

and

$$E_p^y(\mathbf{F}_p) = \{y \in \mathbf{F}_p : (x,y) \in E_p(\mathbf{F}_p)\}.$$

Let $\sum_{[x]} E_p^x(\mathbf{F}_p)$ and $\sum_y E_p^y(\mathbf{F}_p)$ denote the sum of $x-$ and $y-$coordinates of all rational points (x,y) on E_p, respectively. Then we have the following theorem.

Theorem 3.4:

$$\sum_{[x]} E_p^x(\mathbf{F}_p) = \frac{1}{12}\begin{cases} p^3-p & if\ p \equiv 1,7 (mod\, 8) \\ -p^3+12p^2-11p & if\ p \equiv 3,5 (mod\, 8) \end{cases}$$

and

$$\sum_{[x]} E_p^y(\mathbf{F}_p) = \frac{1}{2}\begin{cases} p^2-p & if\ p \equiv 1,7 (mod\, 8), x \in Q_p \\ 0 & if\ p \equiv 1,7 (mod\, 8), x \notin Q_p \\ 0 & if\ p \equiv 3,5 (mod\, 8), x \in Q_p \\ p^2-p & if\ p \equiv 3,5 (mod\, 8), x \notin Q_p \end{cases}$$

for every prime $p \geq 5$.

Proof: Let $U_p = \{1, 2, \cdots, p-1\}$ be the set of units in $\mathbf{F}_p$. Then then taking squares of elements in U_p, we would obtain the set of quadratic residues Q_p. Then it is easily seen that

$$\sum_{x \in Q_p} x = \frac{p^3-p}{24} \quad and \quad \sum_{x \in U_p} x = \frac{p^2-p}{2}.$$

Let $p \equiv 1,7 (mod\, 8)$. Then we know from Theorem 3.3 that $2x$ is a quadratic residue for every $x \in Q_p$, that is, there are two rational points (x,t) and $(x,p-t)$ on E_p. The sum of $x-$coordinates of these two points is $2x$. Therefore the sum of $x-$coordinates of all points (x,y) on E_p is

$$\sum_{[x]} E_p^x(\mathbf{F}_p) = 2\sum_{x \in Q_p} x = \frac{p^3-p}{12}.$$

Now let $p \equiv 3,5 (mod\, 8)$. Then $2x$ is a quadratic residue for every $x \notin Q_p = U_p - Q_p$, that is, there are two rational points (x,t) and $(x,p-t)$ on E_p. The sum of $x-$coordinates of these two points is $2x$. Therefore the sum of all points (x,y) on E_p is

$$\begin{aligned} \sum_{[x]} E_p^x(\mathbf{F}_p) &= 2\left(\sum_{x \in U_p} x - \sum_{x \in Q_p} x\right) \\ &= \frac{-p^3+12p^2-11p}{12}. \end{aligned}$$

Now we consider the sum $\sum_{[y]} E_p^y(\mathbf{F}_p)$. Let $p \equiv 1,7\ (mod\, 8)$ and let $x \in Q_p$. We proved that in this case $2x$ is a quadratic residue and therefore the quadratic congruence $y^2 \equiv 2x (mod\, p)$ has two solutions $y = t$ and $y = p-t$, that is, there are two rational points (x,t) and $(x,p-t)$ on E_p. The sum of $y-$coordinates of these points is p. Recall that there are $\frac{p-1}{2}$ elements x in Q_p such that the quadratic congruence $y^2 \equiv 2x (mod\, p)$ has a solution. So the sum of $y-$coordinates of all points (x,y) on E_p is $p(\frac{p-1}{2}) = \frac{p^2-p}{2}$. Now let $x \notin Q_p$. Then $2x$ is not a quadratic residue. So $y^2 \equiv 2x (mod\, p)$ has no solution. Therefore there is no rational point on E_p. So $\sum_{[y]} E_p^y(\mathbf{F}_p) = 0$. The other cases are similar. ■

REFERENCES

[1] E. Barbeau. *Pell's Equation.* Springer Verlag, 2003.
[2] J. Buchmann and U. Vollmer. *Binary Quadratic Forms: An Algorithmic Approach.* Springer-Verlag, Berlin, Heidelberg, 2007.
[3] D.A. Buell. *Binary Quadratic Forms, Clasical Theory and Modern Computations.* Springer-Verlag, New York, 1989.
[4] H.M. Edwards. *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.E. Flath. *Introduction to Number Theory.* Wiley, 1989.
[6] I. Niven, H.S. Zuckerman and H.L. Montgomery. *An Introduction to the Theory of Numbers.* Fifth Edition, John Wiley&Sons, Inc., New York, 1991.
[7] A. Tekcan. *Pell Equation $x^2 - Dy^2 = 2$, II.* Bulletin of the Irish Math. Soc. **54**(2004), 73–89.
[8] A. Tekcan, O. Bizim and M. Bayraktar. *Solving the Pell Equation using the Fundamental Element of the Field $\mathbf{Q}(\sqrt{\Delta})$.* South East Asian Bulletin of Maths **30**(2)(2006), 355–366.
[9] A. Tekcan. *On the Pell Equation $x^2-(k^2-2)y^2 = 2^t$.* Crux Math.with Mathematical Mayhem **33**(6)(2007), 361–365.
[10] A. Tekcan. *The Pell Equation $x^2 - Dy^2 = \pm 4$.* App. Math. Sci. **1**(8)(2007), 363–369.
[11] A. Tekcan, B. Gezer, and O. Bizim. *On the Integer Solutions of the Pell Equation $x^2 - dy^2 = 2^t$.* Int. Jour. of Math. Sci. **1**(3)(2007), 204–208.
[12] A. Tekcan. *The Cubic Congruence $x^3+ax^2+bx+c \equiv 0(mod\ p)$ and Binary Quadratic Forms $F(x,y) = ax^2+bxy+cy^2$.* Ars Combinatoria **85**(2007), 257–269.
[13] A. Tekcan. *The Pell Equation $x^2 - (k^2-k)y^2 = 2^t$.* Int.Journal of Comp. and Mathematical Sciences **2**(1)(2008), 5–9.