General Mathematics Vol. 18, No. 4 (2010), 3–17

The family of indefinite binary quadratic forms and elliptic curves over finite fields [1]

Arzu Özkoç, Ahmet Tekcan

Abstract

In this paper, we consider some properties of the family of indefinite binary quadratic forms and elliptic curves. In the first section, we give some preliminaries from binary quadratic forms and elliptic curves. In the second section, we define a special family of indefinite forms F_i and then we obtain some properties of these forms. In the third section, we consider the number of rational points on conics C_{F_i} over finite fields. In the last section, we consider the number of rational points on elliptic curves E_{F_i} over finite fields, also we give some formulas for the sum of $x-$and $y-$coordinates of rational points (x, y) on E_{F_i}.

2010 Mathematics Subject Classification:11E04, 11E16, 11G07, 11G20, 14G05

Key words and phrases: Indefinite binary quadratic forms, Conics, Elliptic curves.

1 Preliminaries

A real binary quadratic form (or just a form) F is a polynomial in two variables x and y of the type

$$F = F(x, y) = ax^2 + bxy + cy^2 \tag{1}$$

[1] *Received 27 March, 2008*
Accepted for publication (in revised form) 28 October, 2009

with real coefficients a, b, c. We denote F briefly by $F = (a, b, c)$. The discriminant of F is defined by the formula $b^2 - 4ac$ and is denoted by $\Delta = \Delta(F)$. F is an integral form if and only if $a, b, c \in \mathbb{Z}$, and is indefinite if and only if $\Delta(F) > 0$. An indefinite definite form $F = (a, b, c)$ of discriminant Δ is said to be reduced if $\left|\sqrt{\Delta} - 2|a|\right| < b < \sqrt{\Delta}$. A principal form F of discriminant Δ is a form given by

$$F(x,y) = \begin{cases} x^2 - \frac{\Delta}{4}y^2 & \text{if } \Delta \equiv 0 (\text{mod } 4) \\ x^2 + xy - \frac{\Delta-1}{4}y^2 & \text{if } \Delta \equiv 1 (\text{mod } 4). \end{cases} \tag{2}$$

Note that principal forms are always reduced. Most properties of quadratic forms can be giving by the aid of extended modular group $\overline{\Gamma}$ ([13]). Gauss (1777-1855) defined the group action of $\overline{\Gamma}$ on the set of forms as follows:

$$\begin{aligned} gF(x,y) &= \left(ar^2 + brs + cs^2\right)x^2 + (2art + bru + bts + 2csu)\,xy \\ &\quad + \left(at^2 + btu + cu^2\right)y^2 \end{aligned} \tag{3}$$

for $g = \begin{pmatrix} r & s \\ t & u \end{pmatrix} = [r; s; t; u] \in \overline{\Gamma}$, that is, gF is gotten from F by making the substitution $x \to rx + tu$ and $y \to sx + uy$. Moreover, $\Delta(F) = \Delta(gF)$ for all $g \in \overline{\Gamma}$, that is, the action of $\overline{\Gamma}$ on forms leaves the discriminant invariant. If F is indefinite or integral, then so is gF for all $g \in \overline{\Gamma}$. Let F and G be two forms. If there exists a $g \in \overline{\Gamma}$ such that $gF = G$, then F and G are called equivalent. If $\det g = 1$, then F and G are called properly equivalent and if $\det g = -1$, then F and G are called improperly equivalent. An element $g \in \overline{\Gamma}$ is called an automorphism of F if $gF = F$. If $\det g = 1$, then g is called a proper automorphism of F, and if $\det g = -1$, then g is called an improper automorphism of F. Let $Aut(F)^+$ denote the set of proper automorphisms of F and let $Aut(F)^-$ denote the set of improper automorphisms of F. Let $F = (a, b, c)$ be an indefinite form and let $\Phi = \{[1; s; 0; 1] : s \in \mathbb{Z}\}$. Then Φ is a cyclic subgroup of $\mathrm{SL}(2, \mathbb{Z})$ which is generated by $g = [1; 1; 0; 1]$. Now we want to determine the element in the $\Phi-$orbit of F for which the absolute value of xy is minimal. For $s \in \mathbb{Z}$, we have $g^s F = (a, b + 2sa, as^2 + bs + c)$. Hence the coefficient of x^2 of any form in the $\Phi-$orbit of F is a and the coefficient of xy of such a form is uniquely determined $(\text{mod } 2a)$. If we choose $s = \left\lfloor \frac{a-b}{2a} \right\rfloor$, then we have $-a < b + 2sa \leq a$. This choice of s minimizes the absolute value of b. Further, the coefficient of y^2 in $g^s F$ is $\frac{(2as+b)^2+|\Delta|}{4a}$. So this choice of

s minimizes this coefficient. Hence the form $F = (a, b, c)$ is called normal if $-|a| < b \leq |a|$ for $|a| \geq \sqrt{\Delta}$ or $\sqrt{\Delta} - 2|a| < b < \sqrt{\Delta}$ for $|a| < \sqrt{\Delta}$. We see as above that, the $\Phi-$orbit of F contains one normal form which can be obtained as $g^s F$ with $s = \left\lfloor \frac{a-b}{2a} \right\rfloor$. The normal form in the $\Phi-$orbit of F is called the normalization of F, which means replacing F by its normalization (see [2]). Let $\rho(F)$ denote the normalization of $(c, -b, a)$. Let $F = F_0 = (a_0, b_0, c_0)$ and let

$$s_i = \begin{cases} sign(c_i) \left\lfloor \frac{b_i}{2|c_i|} \right\rfloor & \text{for } |c_i| \geq \sqrt{\Delta} \\ \\ sign(c_i) \left\lfloor \frac{b_i + \sqrt{\Delta}}{2|c_i|} \right\rfloor & \text{for } |c_i| < \sqrt{\Delta} \end{cases} \tag{4}$$

for $i \geq 0$. Then the reduction of F is

$$\rho^{i+1}(F) = (c_i, -b_i + 2c_i s_i, c_i s_i^2 - b_i s_i + a_i) \tag{5}$$

for $i \geq 0$. Then ρ is called the reduction operator for indefinite binary quadratic forms (for further details on binary quadratic forms see [2, 3, 4]).

2 The family of indefinite binary quadratic forms

In [17], we defined a special family of positive definite binary quadratic forms, and then obtained some properties of these forms and also quadratic congruences and singular curves related to these forms. In the present paper, we will define a family of indefinite binary quadratic forms of the type $F = (1, b, c)$ of discriminant Δ and then obtained some properties of these forms. Later, we will consider the number of rational points on conics and elliptic curves related to these forms. First we define the family of indefinite quadratic forms.

Theorem 1 *If $\Delta \equiv 1 (\text{mod } 4)$, say $\Delta = 1 + 4k$ for a positive integer $k \geq 1$, then there exist $k-$indefinite binary quadratic forms of the type*

$$F_i = (1, 2i + 1, i^2 + i - k), \;\; 1 \leq i \leq k \tag{6}$$

of discriminant Δ.

Proof. Let $\Delta \equiv 1 (\text{mod } 4)$, say $\Delta = 1 + 4k$. Then Δ is odd. Let $F_i = (1, b_i, c_i)$ be a given form of discriminant Δ. Since Δ is odd, the coefficient b_i must be

odd. Let $b_i = 2i+1$ for an integer $i \geq 1$. Then

$$c_i = \frac{b_i^2 - \Delta}{4} = \frac{(2i+1)^2 - (1+4k)}{4} = i^2 + i - k.$$

Note that i must be $i \leq k$. Therefore, there are k-indefinite binary quadratic forms $F_i = (1, 2i+1, i^2+i-k)$ of discriminant Δ.

Let $\Im$ denote the family of indefinite binary quadratic forms F_i defined in (6), that is,

$$\Im = \left\{F_i : F_i = (1, 2i+1, i^2+i-k),\ 1 \leq i \leq k\right\}. \tag{7}$$

From now on we assume that F_i is indefinite and $\Delta \equiv 1 (\mathrm{mod}\ 4)$ is a positive non-square discriminant throughout the paper. Now we consider the reduction of F_i. Set

$$\begin{aligned} A_1 &= \{3,4,5\} \\ A_2 &= \{7,8,9,10,11\} \\ A_3 &= \{13,14,15,16,17,18,19\} \\ &\cdots \\ A_i &= \left\{i^2+i+1, i^2+i+2, \cdots, i^2+3i, i^2+3i+1\right\} \end{aligned} \tag{8}$$

for a non-negative integer i. Then $s(A_i) = 2i+1$. If $k = i^2+1$ or $k = i^2 + 3i + 2$, then Δ is a square, that is why we disregard these values of i from A_i. Now we can give the following theorem.

Theorem 2 *Let F_i be a form in $\Im$ of discriminant Δ. Then F_i is reduced if and only if $k \in A_i$ for some i.*

Proof. Let us assume that $F_i = (1, 2i+1, i^2+i-k)$ is reduced. Then $\left|\sqrt{\Delta} - 2|a|\right| < b < \sqrt{\Delta} \Leftrightarrow \left|\sqrt{1+4k} - 2\right| < 2i+1 < \sqrt{1+4k} \Leftrightarrow \sqrt{1+4k} - 2 < 2i+1 < \sqrt{1+4k}$ since $1+4k > 4$. Hence we get $k < i^2+3i+2$ from $\sqrt{1+4k} - 2 < 2i+1$ and $i^2+i < k$ from $2i+1 < \sqrt{1+4k}$. Therefore $i^2+i < k < i^2+3i+2$, that is, $k \in (i^2+i, i^2+i+2)$. So $k \in A_i$.

Let $k \in A_i$. Then $i^2+i < k < i^2+3i+2$, and hence $\sqrt{1+4k} - 2 < 2i+1 < \sqrt{1+4k} \Leftrightarrow \left|\sqrt{\Delta} - 2|a|\right| < b < \sqrt{\Delta}$, that is, F_i is reduced.

We proved in above theorem that the form F_i is reduced if and only if $k \in A_i$. For the other values of i, the forms F_i are not reduced. Therefore there exist exactly one reduced form for each given discriminant Δ. Now we consider the reduction of non-reduced forms by using the reduction algorithm as we mentioned in the previous section. Let $F_j = (1, 2j, j^2 + j - k)$ be a reduced form. Then $k \in A_j$. Let $F_i = F_{i_0} = (1, 2i, i^2 + i - k)$ be any non reduced form for $i \neq j$. Then by (4), we get $s_0 = 0$ and hence by (5), $\rho^1(F_i) = (i^2 + i - k, -2i, 1)$. But $\rho^1(F_i)$ is not reduced since $-2i$ is negative. If we apply the reduction algorithm to $\rho^1(F_i)$ again, then we find that $s_1 = j - i$ and hence $\rho^2(F_i) = (1, 2j, j^2 + i - k)$. This form is reduced. So the reduction type of F_i is $\rho^2(F_i) = (1, 2j, j^2 + i - k)$. In fact, $\rho^2(F_i) = F_j$. Hence we proved the following theorem.

Theorem 3 *The reduction type of F_i is $\rho^2(F_i) = (1, 2j, j^2 + i - k)$.*

Example 1 *Let $\Delta = 53$. Then $k = 13 \in A_3$. So $F_3 = (1, 7, -1)$ is reduced. Non-reduced forms and their reduced types are giving in the following table:*

Table 1: Reduction of F_i

i	F_i	s_0	$\rho^1(F_i)$	s_1	$\rho^2(F_i)$
1	$(1, 3, -11)$	0	$(-11, -3, 1)$	2	$(1, 7, -1)$
2	$(1, 5, -7)$	0	$(-7, -5, 1)$	1	$(1, 7, -1)$
3	$(\mathbf{1, 7, -1})$				
4	$(1, 9, 7)$	0	$(7, -9, 1)$	-1	$(1, 7, -1)$
5	$(1, 11, 17)$	0	$(17, -11, 1)$	-2	$(1, 7, -1)$
6	$(1, 13, 29)$	0	$(29, -13, 1)$	-3	$(1, 7, -1)$
7	$(1, 15, 43)$	0	$(43, -15, 1)$	-4	$(1, 7, -1)$
8	$(1, 17, 59)$	0	$(59, -17, 1)$	-5	$(1, 7, -1)$
9	$(1, 19, 77)$	0	$(77, -19, 1)$	-6	$(1, 7, -1)$
10	$(1, 21, 97)$	0	$(97, -21, 1)$	-7	$(1, 7, -1)$
11	$(1, 23, 119)$	0	$(119, -23, 1)$	-8	$(1, 7, -1)$
12	$(1, 25, 143)$	0	$(143, -25, 1)$	-9	$(1, 7, -1)$
13	$(1, 27, 169)$	0	$(169, -27, 1)$	-10	$(1, 7, -1)$

Now we consider the transforming of F_i into principal forms. Since $\Delta(F_i) \equiv 1 (\text{mod } 4)$, the principal form of discriminant Δ is

$$F = \left(1, 1, \frac{1 - \Delta}{4}\right) \tag{9}$$

by (2). Now we can give the following theorem.

Theorem 4 *Let F_i be the form defined in* (6) *and let F be the principal form defined in* (9). *Then there exists a $g \in \overline{\Gamma}$ such that $gF_i = F$, that is, the form F_i can be transformed into the principal form F.*

Proof. Let $F_i = (1, 2i+1, i^2+i-k)$ and let $g = [r; s; t; u] \in \overline{\Gamma}$. Then we have the following system of equations:

$$\begin{aligned} r^2 + (2i+1)rs + (i^2+i-k)s^2 &= 1 \\ 2rt + (2i+1)ru + (2i+1)ts + 2(i^2+i-k)su &= 1 \\ t^2 + (2i+1)tu + (i^2+i-k)u^2 &= \frac{1-\Delta}{4}. \end{aligned}$$

It is easily seen that this system of equations has a solution for $r = 1, s = 0$, $t = -i$ and $u = 1$ or $r = -1, s = 0, t = i$ and $u = -1$, that is, $gF_i = F$ for $g = \pm[1; 0; -i; 1] \in \overline{\Gamma}$. So F_i can be transformed into the principal form.

Now we consider the proper and improper automorphisms of indefinite forms F_i.

Theorem 5 *Let F_i be the form defined in* (6). *Then*

$$\#Aut(F_i)^+ = \begin{cases} 10 & \text{if } p = 5 \\ 6 & \text{if } p = 12 \text{ and } i = 1, 2 \\ 2 & \text{otherwise} \end{cases}$$

and

$$\#Aut(F_i)^- = \begin{cases} 10 & \text{if } p = 5 \\ 4 & \begin{cases} \text{if } p = 13 \\ \text{if } p = 29 \text{ and } i = 1, 2, 3, 4 \\ \text{if } p = 37 \text{ and } i = 3 \\ \text{if } p = 53 \text{ and } i = 2, 3, 4, 5 \end{cases} \\ 2 & \text{otherwise.} \end{cases}$$

Proof. First we consider the proper automorphisms. Let $p = 5$. Then $F_1 = (1, 3, 1)$. Let $g = [r, s, t, u] \in \overline{\Gamma}$. Then we have the following system of equations:

$$\begin{aligned} r^2 + 3rs + s^2 &= 1 \\ 2rt + 3ru + 3ts + 2su &= 3 \\ t^2 + 3tu + u^2 &= 1. \end{aligned}$$

This system of equations has a solution for $g = \pm[8,-3,3,-1], \pm[3,-1,1,0]$, $\pm[1,0,0,1]$, $\pm[1,-3,3,-8]$ and $\pm[0,1,-1,3]$. So

$$Aut(F_1)^+ = \left\{ \begin{array}{c} \pm[8,-3,3,-1], \pm[3,-1,1,0], \pm[1,0,0,1], \\ \pm[1,-3,3,-8], \pm[0,1,-1,3] \end{array} \right\}.$$

Hence $\#Aut(F_1)^+ = 10$.

For $p = 13$, $Aut(F_1)^+ = \{\pm[10,-3,-3,1], \pm[1,3,3,10], \pm[1,0,0,1]\}$ and $Aut(F_2)^+ = \{\pm[13,-3,9,-2], \pm[2,-3,9,-13], \pm[1,0,0,1]\}$. For the other values of p, we have $Aut(F_i)^+ = \{\pm[1,0,0,1]\}$ for every i.

Now we consider the improper automorphisms. For $p = 5$, $Aut(F_1)^- = \{\pm[3,-1,8,-3], \pm[3,-8,1,-3], \pm[1,0,3,-1], \pm[1,-3,0,-1], \pm[0,1,1,0]\}$.

For $p = 13$, $Aut(F_1)^- = \{\pm[1,3,0,-1], \pm[1,0,3,-1]\}$, $Aut(F_2)^- = \{\pm[2,-3,1,-2], \pm[1,0,5,-1]\}$ and $Aut(F_3)^- = \{\pm[5,-3,8,-5], \pm[1,0,7,-1]\}$.

For $p = 29$, $Aut(F_1)^- = \{\pm[6,5,-7,-6], \pm[1,0,3,-1]\}$, $Aut(F_2)^- = \{\pm[1,5,0,-1], \pm[1,0,5,-1]\}$, $Aut(F_3)^- = \{\pm[4,-5,3,-4], \pm[1,0,7,-1]\}$, $Aut(F_4)^- = \{\pm[9,-5,16,-9], \pm[1,0,9,-1]\}$.

For $p = 37$, $Aut(F_3)^- = \{\pm[11,-24,5,-11], \pm[1,0,7,-1]\}$ and for $p = 53$, $Aut(F_2)^- = \{\pm[8,7,-9,-8], \pm[1,0,5,-1]\}$, $Aut(F_3)^- = \{\pm[1,7,0,-1], \pm[1,0,7,-1]\}$, $Aut(F_4)^- = \{\pm[6,-7,5,-6], \pm[1,0,9,-1]\}$, $Aut(F_5)^- = \{\pm[13,-7,24,-13], \pm[1,0,11,-1]\}$. For other values of p, we have $Aut(F_i)^- = \{\pm[1,0,2i+1,-1]\}$ for every i. This completes the proof.

3 From quadratic forms to conics

In the previous section, we define a family of indefinite binary quadratic forms $F_i = (1, 2i+1, i^2+i-k)$ of discriminant $\Delta \equiv 1 (\mathrm{mod}\ 4)$. In this section, we will consider the number of rational points on conics C_{F_i} related to F_i over finite fields. Recall that a conic is given by an equation $C : a_{11}x^2 + 2a_{12}xy + a_{22}y^2 + 2a_{13}x + 2a_{23}y + a_{33} = 0$ for real numbers a_{ij}. Let $p \equiv 1 (\mathrm{mod}\ 4)$ be a prime number and let $N \in \mathbb{F}_p^*$ be a fixed. Let

$$C_{F_i} : x^2 + (2i+1)xy + (i^2+i-k)y^2 - N = 0 \tag{10}$$

be a conic over $\mathbb{F}_p$ for F_i. Set $C_{F_i}(\mathbb{F}_p) = \{(x,y) \in \mathbb{F}_p \times \mathbb{F}_p : C_{F_i} \equiv N (\mathrm{mod}\, p)\}$. Then we have the following result.

Theorem 6 *Let C_{F_i} be the conic in* (10). *Then*

$$\#C_{F_i}(\mathbb{F}_p) = \begin{cases} 2p & \text{if } N \in Q_p \\ 0 & \text{if } N \notin Q_p, \end{cases}$$

where Q_p denotes the set of quadratic residues.

Proof. 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 $x^2 \equiv t^2 \pmod{p} \Leftrightarrow x \equiv \pm t \pmod{p}$, that is, there are two integer solutions $(t, 0)$ and $(p - t, 0)$. So there are two rational points $(t, 0), (p - t, 0)$ on C_{F_i}. If $x = 0$, then $(i^2 + i - k)y^2 \equiv t^2 \pmod{p} \Leftrightarrow y^2 \equiv \pm\frac{t^2}{i^2+i-k} \pmod{p}$ has two solutions since $\frac{t^2}{i^2+i-k}$ is a square mod p. Let $m^2 = \frac{t^2}{i^2+i-k}$. Then $y^2 \equiv m^2 \pmod{p} \Leftrightarrow y \equiv \pm m \pmod{p}$, that is, there are two rational points $(0, m)$ and $(0, p - m)$ on C_{F_i}. Further it is easily seen that if $x = h$ for some $h \in \mathbb{F}_p^*$, then the congruence $h^2 + (2i + 1)hy + (i^2 + i - k)y^2 \equiv t^2 \pmod{p}$ has a solution $y = y_1$, and if $x = p - h$, then the congruence $(p - h)^2 + (2i + 1)(p - h)y + (i^2 + i - k)y^2 \equiv t^2 \pmod{p}$ has a solution $y = y_2$. So we have six rational points $(0, m), (0, p - m)$, $(h, 0), (h, y_1), (p - h, 0)$ and $(p - h, y_2)$ on C_{F_i}. Set $\mathbb{F}_p^{**} = \mathbb{F}_p - \{0, h, p-h\}$. Then there are $p-3$ points x in $\mathbb{F}_p^{**}$ such that the congruence $x^2 + (2i + 1)xy + (i^2 + i - k)y^2 \equiv t^2 \pmod{p}$ has two solutions. Let $x = u$ be a point in $\mathbb{F}_p^{**}$ such that the congruence $u^2+(2i+1)uy+(i^2+i-k)y^2 \equiv t^2 \pmod{p}$ has two solutions $y = y_3$ and $y = y_4$. Then there are two rational points (u, y_3) and (u, y_4) on C_{F_i}, that is, for each point x in $\mathbb{F}_p^{**}$ such that the congruence $x^2 + (2i + 1)xy + (i^2 + i - k)y^2 \equiv t^2 \pmod{p}$ has two solutions, then there are two rational points on C_{F_i}. Hence there are $2(p - 3) = 2p - 6$ rational points. Consequently there are total $2(p - 3) + 6 = 2p$ rational points on C_{F_i}.

Case 2: Let $N \notin Q_p$. If $y = 0$, then $x^2 \equiv N \pmod{p}$ has no solution, and if $x = 0$, then $(i^2 + i - k)y^2 \equiv N \pmod{p}$ has no solution since $\frac{N}{i^2+i-k}$ is not a square mod p. Therefore there are no rational point on C_{F_i}.

4 From quadratic forms to elliptic curves

In this section, we want to carry out the results we obtained in Section 2 to the elliptic curves. For this reason, we first give some preliminaries on elliptic curves. Mordell began his famous paper [11] with the words "Mathematicians have been familiar with very few questions for so long a period with so little

accomplished in the way of general results, as that of finding the rational points on elliptic curves". The history of elliptic curves is a long one, and exciting applications for elliptic curves continue to be discovered. Recently, important and useful applications of elliptic curves have been found for cryptography [7, 9, 10], for factoring large integers [8], and for primality proving [1, 6]. The mathematical theory of elliptic curves was also crucial in the proof of Fermat's Last Theorem [20].

An elliptic curve E over a finite field $\mathbb{F}_p$ is defined by an equation in the Weierstrass form

$$E : y^2 = x^3 + ax^2 + bx, \tag{11}$$

where $a, b \in \mathbb{F}_p$ and $b^2(a^2 - 4b) \neq 0$ with discriminant $\Delta(E) = 16b^2(a^2 - 4b)$. If $\Delta(E) = 0$, then E is not an elliptic curve, it is a curve of genus 0 (in fact it is a singular curve). We can view an elliptic curve E as a curve in projective plane $\mathbb{P}^2$, with a homogeneous equation $y^2z = x^3 + ax^2z^2 + bxz^3$, and one point at infinity, namely $(0, 1, 0)$. This point ∞ is the point where all vertical lines meet. We denote this point by O. The set of rational points $E(\mathbb{F}_p) = \{(x, y) \in \mathbb{F}_p \times \mathbb{F}_p : y^2 = x^3 + ax^2 + bx\} \cup \{O\}$ on E is a subgroup of E. The order of $E(\mathbb{F}_p)$, denoted by $\#E(\mathbb{F}_p)$, is defined as the number of the points on E and is given by

$$\#E(\mathbb{F}_p) = p + 1 + \sum_{x \in \mathbb{F}_p} \left(\frac{x^3 + ax^2 + bx}{\mathbb{F}_p} \right),$$

where $(\frac{\cdot}{\mathbb{F}_p})$ denotes the Legendre symbol (for the arithmetic of elliptic curves and rational points on them see [12, 19]).

Now we want to construct a connection between quadratic forms and elliptic curves. For this reason, let $F = (a, b, c)$ be a quadratic form of discriminant $\Delta(F) = b^2 - 4ac$. We define the corresponding elliptic curve E_F as

$$E_F : y^2 = ax^3 + bx^2 + cx. \tag{12}$$

If we take $x \to \frac{x}{\sqrt[3]{a}}$ in (12), then we obtain

$$E_F : y^2 = x^3 + ba^{-2/3}x^2 + ca^{-1/3}x. \tag{13}$$

The discriminant of E_F is hence $\Delta(E_F) = 16(\frac{c}{a})^2\Delta(F)$. So we have a correspondence between binary quadratic forms and elliptic curves, that is, we have the following diagram:

$$\begin{array}{ccc} F=(a,b,c) & \rightarrow & E_F : y^2 = x^3 + ba^{-2/3}x^2 + ca^{-1/3}x \\ \downarrow & & \downarrow \\ \Delta(F) & \rightarrow & \Delta(E_F) = 16(\frac{c}{a})^2\Delta(F) \end{array}$$

In [5, 14, 15, 16, 18], we considered some specific elliptic (also singular) curves and derived some results concerning them. In this section, we define a new elliptic curve related to F_i defined in (6). To get this let p be a prime number such that $p \equiv 1(\text{mod } 4)$, say $p = 1 + 4k$ for an integer $k \geq 1$. We set the corresponding elliptic curve as

$$E_{F_i} : y^2 = x^3 + (2i+1)x^2 + (i^2 + i - k)x. \tag{14}$$

Let $E_{F_i}(\mathbb{F}_p) = \left\{(x,y) \in \mathbb{F}_p \times \mathbb{F}_p : x^3 + (2i+1)x^2 + (i^2+i-k)x\right\} \cup \{O\}$. Then we can give the following theorem.

Theorem 7 *Let E_{F_i} be the elliptic curve in* (14). *If $i = 1$, then*

$$\#E_{F_1}(\mathbb{F}_p) = \begin{cases} p & \text{if } p \equiv 1, 5(\text{mod } 24) \\ p+2 & \text{if } p \equiv 13, 17(\text{mod } 24) \end{cases}$$

and if $i = k$, then $\#E_{F_k}(\mathbb{F}_p) = p$ for every prime p.

Proof. Let $i = 1$. Then $F_1 = (1, 3, 2-k)$ and hence $E_{F_1} : y^2 = x^3 + 3x^2 + (2-k)x$. Let $p \equiv 1, 5(\text{mod } 24)$. If $x = 0$, then $y^2 \equiv 0(\text{mod } p) \Leftrightarrow y = 0$. So $(0,0)$ is a rational point on E_{F_1}. If $y = 0$, then $x^3 + 3x^2 + (2-k)x \equiv 0(\text{mod } p) \Leftrightarrow x\left(x^2 + 3x + (2-k)\right) \equiv 0(\text{mod } p)$. Hence $x \equiv 0(\text{mod } p)$ and $x^2 + 3x + (2-k) \equiv 0(\text{mod } p)$. It is easily seen that $x = 0$ and $x = \frac{p-3}{2} = 2k-1$ are solutions since $(2k-1)^2 + 3(2k-1) + (2-k) = k(1+4k) \equiv 0(\text{mod } p)$. So we have two rational points $(0,0)$ and $(\frac{p-3}{2}, 0)$ on E_{F_1}. It is easily seen that $\frac{p-3}{2} \in Q_p$. Let x be a quadratic residue mod p, that is, $(\frac{x}{p}) = 1$. Then $\left(\frac{x^3+3x^2+(2-k)x}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{x-\frac{p-3}{2}}{p}\right) = \left(\frac{x-\frac{p-3}{2}}{p}\right)$. So if $x = \frac{p-3}{2}$, then $\left(\frac{x^3+3x^2+(2-k)x}{p}\right) = 0$. Hence the quadratic congruence $y^2 \equiv 0(\text{mod } p)$ has one solution $y = 0$ as we mentioned above. If $x \neq \frac{p-3}{2}$, then $\left(\frac{x^3+3x^2+(2-k)x}{p}\right) = 1$, that is, $x^3 + 3x^2 + (2-k)x$ is a square mod p. Let $x^3 + 3x^2 + (2-k)x = u^2$ for $u \in \mathbb{F}_p^* = \mathbb{F}_p - \{0\}$. Then $y^2 \equiv u^2(\text{mod } p) \Leftrightarrow y \equiv \pm u(\text{mod } p)$. Hence

there are two points (x,u) and $(x,p-u)$ on E_{F_1}, that is, for every x, there are two points. We know that there are $\frac{p-1}{2}-1=\frac{p-3}{2}$ (we mines 1 from the number of quadratic residues since $x=\frac{p-3}{2}$ is a quadratic residue but for this value of x, there are one solution y, for the other values of x, there are two solutions y) elements x such that $x^3+3x^2+(2-k)x$ a square. Hence there are $2\left(\frac{p-3}{2}\right)=p-3$ points on E_{F_1}. Adding the point ∞, we get total $p-3+2+1=p$ points on E_{F_1}.

Similarly it can be shown that if $p\equiv 13,17(\mathrm{mod}\,24)$, then there are $p+2$ rational points on E_{F_1} and if $i=k$, then there are p rational points on E_{F_k}.

Remark 1 *If $i=1$ then for every $x\notin Q_p$, $\left(\frac{x^3+3x^2+(2-k)x}{p}\right)=-1$ for every prime $p\equiv 1,5(\mathrm{mod}\ 24)$ and $p\equiv 13,17(\mathrm{mod}\ 24)$ also if $i=k$ then for every $x\notin Q_p$, $\left(\frac{x^3+(2k+1)x^2+k^2x}{p}\right)=-1$ for every prime p. Note that in above theorem we only consider the cases $i=1$ and $i=k$. When we consider the other cases, then we found that there are $p+2$ or p rational points on E_{F_i}. But we can not determine for what values of i, E_{F_i} has $p+2$ and for what values of i, E_{F_i} has p rational points.*

Now we consider the sum of $x-$ and $y-$coordinates of all rational points (x,y) on E_{F_i} over $\mathbb{F}_p$. Set $E^x_{F_i}(\mathbb{F}_p)=\{x\in\mathbb{F}_p:(x,y)\in E_{F_i}(\mathbb{F}_p)\}$ and $E^y_{F_i}(\mathbb{F}_p)=\{y\in\mathbb{F}_p:(x,y)\in E_{F_i}(\mathbb{F}_p)\}$ and let $\sum_{[x]}E^x_{F_i}(\mathbb{F}_p)$ and $\sum_{[y]}E^y_{F_i}(\mathbb{F}_p)$ denote the sum of $x-$ and $y-$coordinates of all rational points (x,y) on E_{F_i}, respectively. Then we have following theorems.

Theorem 8 *If $i=1$, then*

$$\sum_{[x]}E^x_{F_1}(\mathbb{F}_p)=\begin{cases}\left(\frac{3p-9}{2}\right).x & \text{if } p\equiv 1,5(\mathrm{mod}\,24)\\ \left(\frac{3p-5}{2}\right).x & \text{if } p\equiv 13,17(\mathrm{mod}\,24)\end{cases}$$

and if $i=k$, then

$$\sum_{[x]}E^x_{F_k}(\mathbb{F}_p)=\left(\frac{5p-13}{4}\right).x$$

for every prime p.

Proof. Let $i=1$. Then $E_{F_1}: y^2=x^3+3x^2+(2-k)x$. We proved in Theorem 7 that there are $\frac{p-3}{2}$ points x such that $x^3+3x^2+(2-k)x$ a

square, that is, $\left(\frac{x^3+3x^2+(2-k)x}{\mathbb{F}_p}\right) = 1$. Therefore there are two points (x, y) and $(x, -y)$. Further $\left(\frac{x^3+3x^2+(2-k)x}{\mathbb{F}_p}\right) = 0$ for $x = \frac{p-3}{2}$, that is, there is one point $(\frac{p-3}{2}, 0)$ on E_{F_1}. So the sum of x-coordinates of all rational points (x, y) on E_{F_1} is $\left[2\left(\frac{p-3}{2}\right) + \frac{p-3}{2}\right].x = \left(\frac{3p-9}{2}\right).x$. Similarly it can be shown that if $p \equiv 13, 17 (\mathrm{mod}\, 24)$, then the sum of x-coordinates of all rational points (x, y) on E_{F_1} is $\left(\frac{3p-5}{2}\right).x$ and if $i = k$, then the sum of x-coordinates of all rational points (x, y) on E_{F_k} is $\left(\frac{5p-13}{4}\right).x$ as we claimed.

From above theorem, we can give the following theorem.

Theorem 9 *If $i = 1$, then*

$$\sum_{[x]} E^x_{F_1}(\mathbb{F}_p) = \begin{cases} \frac{p^3-7p+18}{12} & \text{if } p \equiv 1, 5 (\mathrm{mod}\, 24) \\ \\ \frac{p^3+5p-18}{12} & \text{if } p \equiv 13, 17 (\mathrm{mod}\, 24) \end{cases}$$

and if $i = k$, then

$$\sum_{[x]} E^x_{F_k}(\mathbb{F}_p) = \frac{p^3 - 4p + 3}{12}$$

for every prime p.

Proof. Let $U_p = \{1, 2, \cdots, p-1\}$ be the set of units in $\mathbb{F}_p$. Then taking squares of elements in U_p, we would obtain the set of quadratic residues $Q_p = \left\{1, 4, 9, \cdots, (\frac{p-1}{2})^2\right\}$. Then the sum of all elements in Q_p is $1 + 4 + 9 + \cdots + (\frac{p-1}{2})^2 = \frac{p(p-1)(p+1)}{24}$.

Now let $i = 1$. Then $E_{F_1} : y^2 = x^3 + 3x^2 + (2-k)x$. Let $p \equiv 1, 5 (\mathrm{mod}\ 24)$. Then we know that $\frac{p-3}{2} \in Q_p$, but for this value there is one point $(\frac{p-3}{2}, 0)$ on E_{F_1}. Also $(0, 0)$ on E_{F_1}. Let $H = Q_p - \{\frac{p-3}{2}\}$. Then the sum of all elements in H is hence $\frac{p(p-1)(p+1)}{24} - \frac{p-3}{2}$. Let $x \in H$. Then $x^3 + 3x^2 + (2-k)x$ is a square, say $x^3 + 3x^2 + (2-k)x = t^2$. Then $y^2 \equiv t^2 (\mathrm{mod}\ p)$. So there are two rational points (x, t) and $(x, p-t)$. The sum of x-coordinates of these two points is $2x$, that is, for every $x \in H$, the sum of x-coordinates of two points (x, t) and $(x, p-t)$ is $2x$. So the sum of x-coordinates of all points on E_{F_1} is $2\left(\frac{p(p-1)(p+1)}{24} - \frac{p-3}{2}\right)$. Further as we said above, the point $(\frac{p-3}{2}, 0)$ is also on E_{F_1}. So

$$\sum_{[x]} E^x_{F_1}(\mathbb{F}_p) = 2\left(\frac{p(p-1)(p+1)}{24} - \frac{p-3}{2}\right) + \frac{p-3}{2} = \frac{p^3 - 7p + 18}{12}.$$

Similarly it can be shown that if $p \equiv 13, 17(\text{mod}24)$, then $\sum\limits_{[x]} E^x_{F_1}(\mathbb{F}_p) = \frac{p^3+5p-18}{12}$ and if $i = k$, then $\sum\limits_{[x]} E^x_{F_k}(\mathbb{F}_p) = \frac{p^3-4p+3}{12}$.

Theorem 10 *If $i = 1$, then*

$$\sum_{[y]} E^y_{F_1}(\mathbb{F}_p) = \begin{cases} \frac{p^2-3p}{2} & \text{if } p \equiv 1, 5(\text{mod } 24) \\ \\ \frac{p^2-p}{2} & \text{if } p \equiv 13, 17(\text{mod } 24) \end{cases}$$

and if $i = k$, then

$$\sum_{[y]} E^y_{F_k}(\mathbb{F}_p) = \frac{p^2 - 3p}{2}$$

for every prime p.

Proof. Let $p \equiv 1, 5(\text{mod } 24)$ and let $i = 1$. Then $E_{F_1} : y^2 = x^3+3x^2+(2-k)x$. Then we know from Theorem 7 that there are $\frac{p-3}{2}$ points x such that $x^3+3x^2+(2-k)x$ a square, that is, $\left(\frac{x^3+3x^2+(2-k)x}{\mathbb{F}_p}\right) = 1$. Let $x^3 + 3x^2 + (2-k)x = t^2$ for some integer $t \neq 0$. Then the quadratic congruence $y^2 \equiv t^2(\text{mod}\, p) \Leftrightarrow y \equiv \pm t(\text{mod}\, p)$ has two solutions $y = t$ and $y = -t = p - t$. The sum of these values of y is p. We know that there are $\frac{p-3}{2}$ points x such that $x^3 + 3x^2 + (2-k)x$ a square. So the sum of $y-$coordinates of all points (x, y) on E_{F_1} is $p(\frac{p-3}{2}) = \frac{p^2-3p}{2}$.

Similarly it can be shown that if $p \equiv 13, 17(\text{mod}\, 24)$, then the sum of $y-$coordinates of all points (x, y) on E_{F_1} is $\frac{p^2-p}{2}$ and if $i = k$, then the sum of $y-$coordinates of all points (x, y) on E_{F_k} is $\frac{p^2-3p}{2}$.

References

[1] A.O.L. Atkin and F. Moralin, *Elliptic Curves and Primality Proving,* Math. Computation 61, 1993, 29–68.

[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] D.E. Flath, *Introduction to Number Theory,* Wiley, 1989.

[5] B. Gezer, H. Özden, A. Tekcan and O. Bizim, *The Number of Rational Points on Elliptic Curves* $y^2 = x^3 + b^2$ *over Finite Fields,* Int. Jour. of Math. Sci. 1, No: 3, 2007, 178–184.

[6] S. Goldwasser and J. Kilian, *Almost all Primes can be Quickly Certified,* In Proc. 18th STOC, Berkeley, May 28-30, 1986, ACM, New York (1986), 316-329.

[7] N. Koblitz, *A Course in Number Theory and Cryptography,* Springer-Verlag, 1994.

[8] H.W.Jr. Lenstra, *Factoring Integers with Elliptic Curves,* Annals of Maths. 126, No: 2, 1987, 649–673.

[9] V.S. Miller, *Use of Elliptic Curves in Cryptography, in Advances in Cryptology–CRYPTO'85,* Lect. Notes in Comp. Sci. 218, Springer-Verlag, Berlin (1986), 417–426.

[10] R.A. Mollin, *An Introduction to Cryptography,* Chapman&Hall/CRC, 2001.

[11] L.J. Mordell, *On the Rational Solutions of the Indeterminate Equations of the Third and Fourth Degrees,* Proc. Cambridge Philos. Soc. 21, 1922, 179–192.

[12] J.H. Silverman, *The Arithmetic of Elliptic Curves,* Springer-Verlag, 1986.

[13] A. Tekcan and O. Bizim, *The Connection between Quadratic Forms and the Extended Modular Group,* Mathematica Bohemica 128, No:3, 2003, 225–236.

[14] A. Tekcan, *The Elliptic Curves* $y^2 = x^3 - t^2x$ *over* $\mathbb{F}_p$*,* Int. Jour. of Comp. Math. Sci., 1, No: 3, 2007, 165–171.

[15] A. Tekcan, *The Number of Rational Points on Singular Curves* $y^2 = x(x-a)^2$ *over Finite Fields* $\mathbb{F}_p$*,* Int. Jour. of Comp.and Math. Sci. 3, No: 1, 2009, 14–17.

[16] A. Tekcan, *The Elliptic Curves* $y^2 = x^3 - 1728x$ *over Finite Fields,* Journal of Alg. Number Theor. Adv. and App. 1, No: 1, 2009, 61–74.

[17] A.Tekcan and A.Özkoç, *Positive Definite Binary Quadratic Forms, Quadratic Congruences and Singular Curves,* Comptes ren.math.-Math.Reports 31, No: 2, 2009, 53–64.

[18] A. Tekcan, *The Elliptic Curves* $y^2 = x(x-1)(x-\lambda)$*,* Accepted for publication to Ars Combinatoria.

[19] L.C. Washington, *Elliptic Curves, Number Theory and Cryptography,* Chapman&Hall /CRC, Boca London, New York, Washington DC, 2003.

[20] A. Wiles, *Modular Elliptic Curves and Fermat's Last Theorem,* Annals of Maths. 141, No: 3, 1995, 443–551.

Arzu Özkoç, Ahmet Tekcan
Uludag University, Faculty of Science
Department of Mathematics
Görükle 16059. Bursa, Turkiye
e-mail: aozkoc@uludag.edu.tr, tekcan@uludag.edu.tr
http://matematik.uludag.edu.tr/AhmetTekcan.htm