Novi Sad J. Math.
Vol. 38, No. 2, 2008, 71-81

ELLIPTIC CURVES, CONICS AND CUBIC CONGRUENCES ASSOCIATED WITH INDEFINITE BINARY QUADRATIC FORMS

Ahmet Tekcan[1], Arzu Özkoç[1], Betül Gezer[1], Osman Bizim[1]

Abstract. In this paper we consider elliptic curves, conics and cubic congruences over finite fields associated with indefinite binary quadratic forms F_i in the proper cycle of $F = (1, 7, -6)$. We determine the number of rational points on elliptic curves $E_{F_i} : y^2 = a_i x^3 + b_i x^2 + c_i x$ and conics $C_{F_i} : a_i x^2 + b_i xy + c_i y^2 - N = 0$ over $\mathbb{F}_{73}$, where $N \in \mathbb{F}_{73}^*$ and $F_i = (a_i, b_i, c_i)$ be any form in the proper cycle of F. In the last section, we consider the number integer solutions of cubic congruences $C^3_{F_i} : x^3 + a_i x^2 + b_i x + c_i \equiv 0 (\bmod 73)$ associated with F_i.

AMS Mathematics Subject Classification (2000): 11E04, 11E12, 11E16, 11D25, 11D79

Key words and phrases: Binary quadratic forms, cubic congruences, elliptic curves, conics

1. Preliminaries

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

$$F = F(x, y) = ax^2 + bxy + cy^2$$

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 quadratic form $F = (a, b, c)$ of discriminant Δ is said to be reduced if

$$\left|\sqrt{\Delta} - 2|a|\right| < b < \sqrt{\Delta}.$$

Most properties of quadratic forms can be given with the aid of extended modular group $\overline{\Gamma}$ (see [18]). Gauss defined the group action of $\overline{\Gamma}$ on the set of forms as follows:

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

[1]Uludag University, Faculty of Science, Department of Mathematics, Görükle, 16059, Bursa, Turkey
e-mails: tekcan@uludag.edu.tr, aozkoc@uludag.edu.tr, betulgezer@uludag.edu.tr, obizim@uludag.edu.tr; `http://matematik.uludag.edu.tr/AhmetTekcan.htm`

for $g = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in \overline{\Gamma}$. Hence two forms F and G are called equivalent if and only if there exists a $g \in \overline{\Gamma}$ such that $gF = G$. 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. If a form F is improperly equivalent to itself, then it is called ambiguous (for further details on binary quadratic forms see [3, 4, 7]).

Let $\rho(F)$ denote the normalization of $(c, -b, a)$. To be more explicit, we set

$$\rho(F) = (c, -b + 2cs, cs^2 - bs + a),$$

where

$$r = r(F) = \begin{cases} sign(c) \left\lfloor \frac{b}{2|c|} \right\rfloor & \text{for } |c| \geq \sqrt{\Delta} \\ \\ sign(c) \left\lfloor \frac{b+\sqrt{\Delta}}{2|c|} \right\rfloor & \text{for } |c| < \sqrt{\Delta}. \end{cases}$$

If F is reduced, then $\rho(F)$ is also reduced. In fact, ρ is a permutation of the set of all reduced indefinite forms. Now, consider the following transformation

$$\tau(F) = \tau(a, b, c) = (-a, b, -c).$$

Then the cycle of F is the sequence $((\tau\rho)^i(G))$ for $i \in \mathbb{Z}$, where $G = (k, l, m)$ is a reduced form with $k > 0$, which is equivalent to F and the proper cycle of F is the sequence $(\rho^i(G))$ for $i \in \mathbb{Z}$, where G is a reduced form which is properly equivalent to F. The cycle and the proper cycle of F are invariants of the equivalence class of F. We represent the cycle or proper cycle of F by its period $F_0 \sim F_1 \sim \cdots \sim F_{l-1}$ of length l. We explain how to compute the cycle and proper cycle of F by the following lemma.

Lemma 1.1. *Let $F = (a, b, c)$ be an indefinite reduced quadratic form of the discriminant Δ. Then the cycle of F is $F_0 \sim F_1 \sim F_2 \sim \cdots \sim F_{l-1}$ of length l, where $F_0 = F = (a_0, b_0, c_0)$,*

$$s_i = |s(F_i)| = \left\lfloor \frac{b_i + \sqrt{\Delta}}{2|c_i|} \right\rfloor \tag{1.1}$$

and

$$F_{i+1} = (a_{i+1}, b_{i+1}, c_{i+1}) = \left(|c_i|,\ -b_i + 2s_i|c_i|,\ -(a_i + b_i s_i + c_i s_i^2)\right) \tag{1.2}$$

for $1 \leq i \leq l-2$. If l is odd, then the proper cycle of F is

$$\begin{aligned} &F_0 \sim \tau(F_1) \sim\ F_2 \sim \tau(F_3) \sim \cdots \sim \tau(F_{l-2}) \sim\ F_{l-1} \\ &\sim \tau(F_0) \sim\ F_1 \sim \tau(F_2) \sim \cdots \sim F_{l-2} \sim \tau(F_{l-1}) \end{aligned}$$

of length $2l$ and if l is even, then the proper cycle of F is

$$F_0 \sim \tau(F_1) \sim\ F_2 \sim \tau(F_3) \sim \ldots \sim F_{l-2} \sim \tau(F_{l-1})$$

of length l. In this case the equivalence class of F is the disjoint union of the proper equivalence class of F and the proper equivalence class of $\tau(F)$ [3].

2. Indefinite Binary Quadratic Forms

In this section we will derive the cycle and proper cycle of an indefinite binary quadratic form $F = (1, 7, -6)$ of the discriminant $\Delta = 73$ which we will need in the later sections.

Theorem 2.1. *Let $F = (1, 7, -6)$. Then the cycle of F is*

$$\begin{aligned} &F_0 = (1,7,-6) \sim F_1 = (6,5,-2) \sim F_2 = (2,7,-3) \\ &\sim F_3 = (3,5,-4) \sim F_4 = (4,3,-4) \sim F_5 = (4,5,-3) \\ &\sim F_6 = (3,7,-2) \sim F_7 = (2,5,-6) \sim F_8 = (6,7,-1) \end{aligned}$$

of length 9*, and the proper cycle of F is*

$$\begin{aligned} &F_0 = (1,7,-6) \sim F_1 = (-6,5,2) \sim F_2 = (2,7,-3) \\ &\sim F_3 = (-3,5,4) \sim F_4 = (4,3,-4) \sim F_5 = (-4,5,3) \\ &\sim F_6 = (3,7,-2) \sim F_7 = (-2,5,6) \sim F_8 = (6,7,-1) \\ &\sim F_9 = (-1,7,6) \sim F_{10} = (6,5,-2) \sim F_{11} = (-2,7,3) \\ &\sim F_{12} = (3,5,-4) \sim F_{13} = (-4,3,4) \sim F_{14} = (4,5,-3) \\ &\sim F_{15} = (-3,7,2) \sim F_{16} = (2,5,-6) \sim F_{17} = (-6,7,1) \end{aligned} \tag{2.1}$$

of length 18*.*

Proof. Let $F = F_0 = (1, 7, -6)$. Then by (1.1), we get $s_0 = 1$ and hence by (1.2), we obtain $F_1 = (6, 5, -2)$. Similarly, we can obtain the following table:

i	1	2	3	4	5	6	7	8	9
a_i	1	6	2	3	4	4	3	2	6
b_i	7	5	7	5	3	5	7	5	7
c_i	-6	-2	-3	-4	-4	-3	-2	-6	-1
s_i	1	3	2	1	1	2	3	1	7

Therefore the cycle of F is $F_0 = (1,7,-6) \sim F_1 = (6,5,-2) \sim F_2 = (2,7,-3) \sim F_3 = (3,5,-4) \sim F_4 = (4,3,-4) \sim F_5 = (4,5,-3) \sim F_6 = (3,7,-2) \sim F_7 = (2,5,-6) \sim F_8 = (6,7,-1)$ of length 9. So by Lemma 1.1, the proper cycle of F is $F_0 = (1,7,-6) \sim F_1 = (-6,5,2) \sim F_2 = (2,7,-3) \sim F_3 = (-3,5,4) \sim F_4 = (4,3,-4) \sim F_5 = (-4,5,3) \sim F_6 = (3,7,-2) \sim F_7 = (-2,5,6) \sim F_8 = (6,7,-1) \sim F_9 = (-1,7,6) \sim F_{10} = (6,5,-2) \sim F_{11} = (-2,7,3) \sim F_{12} = (3,5,-4) \sim F_{13} = (-4,3,4) \sim F_{14} = (4,5,-3) \sim F_{15} = (-3,7,2) \sim F_{16} = (2,5,-6) \sim F_{17} = (-6,7,1)$ of length 18. □

3. Elliptic Curves and Conics

In this section we will consider the number of rational points on the elliptic curves

$$E_{F_i} : y^2 = a_i x^3 + b_i x^2 + c_i x$$

and conics

$$C_{F_i} : a_i x^2 + b_i xy + c_i y^2 - N = 0$$

over $\mathbb{F}_{73}$, where $N \in \mathbb{F}_{73}^*$ and $F_i = a_i x^2 + b_i xy + c_i y^2$ are any form in the proper cycle $F_0 \sim F_1 \sim \cdots \sim F_{17}$ of F obtained in (2.1).

3.1. 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 (see [10, 13, 23]), for factoring large integers (see [11]), and for primality proving (see [1]). The mathematical theory of elliptic curves was also crucial in the proof of Fermat's Last Theorem (see [24]). Recall that an equation of the form

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \tag{3.1}$$

is called an elliptic curve, where $a_1, a_2, a_3, a_4, a_6 \in \mathbb{F}_p$ for prime p. Set

$$\begin{aligned} b_2 &= a_1^2 + 4a_2 \\ b_4 &= 2a_4 + a_1 a_3 \\ b_6 &= a_3^2 + 4a_6 \\ b_8 &= a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2 \\ c_4 &= b_2^2 - 24b_4 \\ c_6 &= -b_2^3 + 36b_2 b_4 - 216b_6. \end{aligned}$$

Then the discriminant of (3.1) is $\Delta = -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6$. We can transform (3.1) to an elliptic curve (called Weierstrass short form)

$$E : y^2 = ax^3 + bx^2 + cx, \tag{3.2}$$

where $a, b, c \in \mathbb{F}_p$. Hence we can view an elliptic curve E as a curve in projective plane $\mathbb{P}^2$ with a homogeneous equation $y^2 z = ax^3 + bx^2 z^2 + cxz^3$, 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

$$E(\mathbb{F}_p) = \{(x, y) \in \mathbb{F}_p \times \mathbb{F}_p : y^2 = ax^3 + bx^2 + cx\} \cup \{O\}$$

on E is a subgroup of E. The order of $E(\mathbb{F}_p)$ is defined as the number of the points on E and is denoted by $\#E(\mathbb{F}_p)$ (for further details on arithmetic of elliptic curves see [15, 23]).

In [8, 9, 20, 22], we considered the number of rational points on elliptic curves over finite fields. We also obtained some results concerning the sum of x- and

y-coordinates of all points (x, y) on these elliptic curves. In this subsection, we will consider the same problem for the elliptic curves

$$E_{F_i} : y^2 = a_i x^3 + b_i x^2 + c_i x \tag{3.3}$$

over $\mathbb{F}_{73}$, where F_i is any form in the proper cycle of F. Let

$$E_{F_i}(\mathbb{F}_{73}) = \{(x, y) \in \mathbb{F}_{73} \times \mathbb{F}_{73} : y^2 = a_i x^3 + b_i x^2 + c_i x\} \cup \{O\}.$$

Then we can give the following theorem.

Theorem 3.1. *Let E_{F_i} be an elliptic curve in* (3.3). *Then*

$$\#E_{F_i}(\mathbb{F}_{73}) = \begin{cases} 73 & \textit{if } i = 4, 13 \\ 75 & \textit{otherwise.} \end{cases}$$

Proof. Let $i = 4, 13$ Consider the elliptic curve $E_i : y^2 = a_i x^3 + b_i x^2 + c_i x$ over $\mathbb{F}_{73}$. If $y = 0$, then we have

$$a_i x^3 + b_i x^2 + c_i x \equiv 0 (\operatorname{mod} 73) \Leftrightarrow x(a_i x^2 + b_i x + c_i) \equiv 0 (\operatorname{mod} 73).$$

So we get

$$x \equiv 0 (\operatorname{mod} 73) \tag{3.4}$$

and

$$a_i x^2 + b_i x + c_i \equiv 0 (\operatorname{mod} 73). \tag{3.5}$$

Hence it is easily seen that $x = 0$ is a solution of (3.4) and

$$x = \begin{cases} 27 & \text{if } i = 4 \\ 46 & \text{if } i = 13 \end{cases}$$

is a solution of (3.5). Therefore if $i = 4$, then there are two rational points $(0, 0)$ and $(17, 0)$ on E_{F_4} and if $i = 13$, then there are two rational points $(0, 0)$ and $(46, 0)$ on $E_{F_{13}}$.

Let Q_p denote the set of quadratic residues. Then

$$\begin{aligned} Q_{73} = \{&1, 2, 3, 4, 6, 8, 9, 12, 16, 18, 19, 23, 24, 25, \mathbf{27}, 32, 35, 36, 37, \\ &38, 41, \mathbf{46}, 48, 49, 50, 54, 55, 57, 61, 64, 65, 67, 69, 70, 71, 72\}. \end{aligned}$$

Note that $27, 46 \in Q_{73}$. Now let

$$Q_{73}^x = Q_{73} - \begin{cases} \{27\} & \text{if } i = 4 \\ \{46\} & \text{if } i = 13. \end{cases}$$

Then it is easily seen that every element of Q_{73}^x makes $a_i x^3 + b_i x^2 + c_i x$ a square (as above we see that $x = 27$ and $x = 46$ make it zero). Let $a_i x^3 + b_i x^2 + c_i x = t^2$ for some $t \in Q_{73}^x$. Then $y^2 \equiv t^2 (\operatorname{mod} 73) \Leftrightarrow y \equiv \pm t (\operatorname{mod} 73)$. Hence, there are two rational points (x,t) and $(x,-t)$ on E_{F_i}, that is, for each point $x \in Q_{73}^x$, there are two points on E_{F_i}. We know that there are 35 elements in Q_{73}^x and each of them makes $a_ix^3+b_ix^2+c_ix$ a square. Therefore there are $2.35=70$ rational points on E_{F_i}. Adding the points $(0,0)$, $(x,0)$ and ∞, we get a total $70+2+1=73$ rational points on E_{F_i}.

Now let $i \neq 4,13$. If $y=0$, then $x=0$ is a solution of (3.4) and

$$x=\begin{cases} 33 & \text{if } i=0 \\ 43 & \text{if } i=1 \\ 53 & \text{if } i=2 \\ 13 & \text{if } i=3 \\ 28 & \text{if } i=5 \\ 11 & \text{if } i=6 \\ 56 & \text{if } i=7 \\ 42 & \text{if } i=8 \\ 40 & \text{if } i=9 \\ 30 & \text{if } i=10 \\ 20 & \text{if } i=11 \\ 60 & \text{if } i=12 \\ 45 & \text{if } i=14 \\ 62 & \text{if } i=15 \\ 17 & \text{if } i=16 \\ 31 & \text{if } i=17 \end{cases}$$

is a solution of (3.5). Hence there are two types of points, $(0,0)$ and $(x,0)$ on E_{F_i}, where x is defined as above. Note that all these values of x are not in Q_{73}. It is easily seen that every element of Q_{73} makes $a_ix^3+b_ix^2+c_ix$ a square. Let $a_ix^3+b_ix^2+c_ix=t^2$ for some $t \in Q_{73}$. Then $y^2 \equiv t^2 (\operatorname{mod} 73) \Leftrightarrow y \equiv \pm t (\operatorname{mod} 73)$. Hence there are two rational points (x,t) and $(x,-t)$ on E_{F_i}, that is, for every point $x \in Q_{73}$, there are two points on E_{F_i}. We know that there are 36 elements in Q_{73}, and each of them makes $a_ix^3+b_ix^2+c_ix$ a square. Therefore there are $2.36=72$ rational points on E_{F_i}. Adding the points $(0,0)$, $(x,0)$ and ∞, we get total $72+2+1=75$ rational points on E_{F_i}. □

3.2. Conics

A conic is given by an equation

$$C: a_{11}x^2+2a_{12}xy+a_{22}y^2+2a_{13}x+2a_{23}y+a_{33}=0 \tag{3.6}$$

for real numbers a_{ij}. Let

$$\delta=\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix}.$$

If $\delta>0$, then C represents an ellipse, if $\delta<0$, then C represents a hyperbola, and if $\delta=0$, then C represents a parabola.

In [21], we considered the number of rational points on the conics $C_{p,k}$: $x^2 - ky^2 = 1$ over finite fields $\mathbb{F}_p$ for $k \in \mathbb{F}_p^*$. In this subsection we will determine the number of rational points on the conics

$$C_{F_i} : a_i x^2 + b_i xy + c_i y^2 - N = 0 \tag{3.7}$$

over $\mathbb{F}_{73}$, where $N \in \mathbb{F}_{73}^*$ and F_i are any form in the proper cycle of F. Let

$$C_{F_i}(\mathbb{F}_{73}) = \{(x, y) \in \mathbb{F}_{73} \times \mathbb{F}_{73} : C_{F_i} : a_i x^2 + b_i xy + c_i y^2 - N \equiv 0 (\text{mod}\, 73)\}.$$

Then we have the following result.

Theorem 3.2. *Let C_{F_i} be the conic in* (3.7)*. Then*

$$\#C_{F_i}(\mathbb{F}_{73}) = \begin{cases} 2p & \text{if } N \in Q_{73} \\ 0 & \text{if } N \notin Q_{73}. \end{cases}$$

Proof. We have two cases:

Case 1: Let $N \in Q_{73}$, say $N = t^2$ for $t \in \mathbb{F}_{73}^*$. If $y = 0$, then

$$a_i x^2 \equiv t^2 (\text{mod}\, 73) \Leftrightarrow x \equiv \pm \frac{t}{\sqrt{a_i}} (\text{mod}\, 73). \tag{3.8}$$

Let $\frac{t}{\sqrt{a_i}} \equiv m(\text{mod}\, 73)$. Then there are two integer solutions $(m, 0)$ and $(p-m, 0)$ of (3.8). So there are two rational points $(m, 0), (p - m, 0)$ on C_{F_i}. If $x = 0$, then

$$c_i y^2 \equiv t^2 (\text{mod } 73) \Leftrightarrow y \equiv \pm \frac{t^2}{\sqrt{c_i}} (\text{mod } 73). \tag{3.9}$$

Let $\frac{t^2}{\sqrt{c_i}} \equiv k(\text{mod}\, 73)$. Then there are solutions $(0, k)$ and $(0, p - k)$ of (3.9) and hence there are two rational points $(0, k)$ and $(0, p - k)$ on C_{F_i}. Further, it is easily seen that if $x = h$ for some $h \in \mathbb{F}_{73}^*$, then the congruence $a_i h^2 + b_i hy + c_i y^2 \equiv t^2 (\text{mod } 73)$ has a solution $y = y_1$, and if $x = p - h$, then the congruence $a_i (p-h)^2 + b_i (p-h) y + c_i y^2 \equiv t^2 (\text{mod } 73)$ has a solution $y = y_2$. So we have six rational points $(m, 0), (p - m, 0), (0, k), (0, p - k), (h, y_1)$ and $(p - h, y_2)$ on C_{F_i}. Now set $G_p = \mathbb{F}_p - \{0, m, h\}$. Then there are $p - 3$ points $x \in G_p$ such that the congruence $a_i x^2 + b_i xy + c_i y^2 \equiv t^2 (\text{mod } 73)$ has two solutions. Let $x = u$ be a point in G_p such that the congruence $a_i u^2 + b_i uy + c_i y^2 \equiv t^2 (\text{mod } 73)$ 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 G_p, there are two rational points on C_{F_i}. Hence there are $2(p - 3) = 2p - 6$ rational points. We see, as above that there are six rational points $(m, 0), (p - m, 0), (0, k), (0, p - k), (h, y_1)$ and $(p - h, y_2)$ on C_{F_i}. Consequently, there are a total $2(p - 3) + 6 = 2p$ of rational points on C_{F_i}.

Case 2: Let $N \notin Q_{73}$. If $y = 0$, then $a_i x^2 \equiv N(\text{mod } 73)$ has no solution since $\frac{N}{a_i}$ is not a square mod 73 and if $x = 0$, then $c_i y^2 \equiv N(\text{mod } 73)$ has no solution since $\frac{N}{c_i}$ is not a square mod 73. Set $H_p = \mathbb{F}_p - \{0\}$. Then there is no point x in H_p such that the congruence $a_ix^2 + b_ixy + c_iy^2 \equiv N(\text{mod } 73)$ has a solution y. Therefore there are no rational points on C_{F_i}. □

Remark 3.3. *Note that in above theorem we only consider the number of rational points on* C_{F_i} *over* $\mathbb{F}_{73}$. *When we consider this problem for other primes* p, *then we can give the following theorem.*

Theorem 3.4. *Let* C_{F_i} *be the conic in* (3.7). *Then*

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

for every prime p *such that* $p \equiv 1(\text{mod } 4)$.

Proof. This theorem can be proved the same way as Theorem 3.2. □

4. Cubic Congruences

In 1896, Voronoi [17] presented his algorithm for computing a system of fundamental units of a cubic number field. His technique was described in terms of binary quadratic forms. Later his technique was restarted in the language of multiplicative lattices by Delone and Faddeev [5]. In 1985, Buchmann [2] generalized the Voronoi's algorithm. A cubic congruence over a field $\mathbb{F}_p$ is

$$x^3 + ux^2 + vx + w \equiv 0(\text{mod}\, p), \tag{4.1}$$

where $u, v, w \in \mathbb{F}_p$. Solutions of cubic congruence (including cubic residues) considered by many authors. Dietmann [6] considered the small solutions of additive cubic congruences. Manin [12] considered the cubic congruence on prime modules. Mordell [14] considered the cubic congruence in three variables and also the congruence $ax^3+by^3+cz^3+dxyz \equiv n(\text{mod}\, p)$. Williams and Zarnke [25] gave some algorithms for solving the cubic congruence on prime modules. Let $H(\Delta)$ denote the group of classes of primitive, integral binary quadratic forms $F(x,y) = ax^2 + bxy + cy^2$ of discriminant Δ. Let K be a quadratic field $\mathbb{Q}(\sqrt{\Delta})$, let L be the splitting field of $x^3 + ax^2 + bx + c$, let $f_0 = f_0(L/K)$ be the part of the conductor of the extension L/K, and let f be a positive integer with $f_0|f$. In [16], Spearman and Williams considered the cubic congruence $x^3+ax^2+bx+c \equiv 0(\text{mod}\, p)$ and binary quadratic forms $F(x,y) = ax^2+bxy+cy^2$. They proved that the cubic congruence $x^3 + ax^2 + bx + c \equiv 0(\text{mod}\, p)$ has three solutions if and only if p is represented by a quadratic form F in J, where $J = J(L,K,F)$ is a subgroup of index 3 in $H(\Delta(K)f^2)$.

In [19, 20], we considered the number of integer solutions of cubic congruences $x^3 + ax^2 + bx + c \equiv 0(\text{mod } p)$ for binary quadratic forms $F(x,y) =$

$ax^2 + bxy + cy^2$. In this section we will consider the same problem for cubic congruences

$$C^3_{F_i} : x^3 + a_i x^2 + b_i x + c_i \equiv 0 (\text{mod } 73) \tag{4.2}$$

associated with $F_i = a_i x^2 + b_i xy + c_i y^2$, which is a form in the proper cycle of F. Let

$$C^3_{F_i}(\mathbb{F}_{73}) = \{x \in \mathbb{F}_{73} : x^3 + a_i x^2 + b_i x + c_i \equiv 0 (\text{mod } 73)\}.$$

Then we have the following theorem.

Theorem 4.1. *Let $C^3_{F_i}$ be the cubic congruence in* (4.2). *Then*

$$\#C^3_{F_i}(\mathbb{F}_{73}) = \begin{cases} 3 & \textit{if } i = 5, 6, 8, 14, 15, 17 \\ 1 & \textit{if } i = 0, 4, 9, 13 \\ 0 & \textit{otherwise.} \end{cases}$$

Proof. Let $i = 5$. Then $F_5 = (-4, 5, 3)$ by (2.1). It is easily seen that the cubic congruence

$$C^3_{F_5} : x^3 - 4x^2 + 5x + 3 \equiv 0 (\text{mod } 73)$$

has three solutions $x = 32, 54, 64$. In fact one can obtain the following table:

i	F_i	$C^3_{F_i}$	$C^3_{F_i}(\mathbb{F}_{73})$	$\#C^3_{F_i}(\mathbb{F}_{73})$
0	F_0	$x^3 + x^2 + 7x - 6$	{41}	1
1	F_1	$x^3 - 6x^2 + 5x + 2$	{}	0
2	F_2	$x^3 + 2x^2 + 7x - 3$	{}	0
3	F_3	$x^3 - 3x^2 + 5x + 4$	{}	0
4	F_4	$x^3 + 4x^2 + 3x - 4$	{12}	1
5	F_5	$x^3 - 4x^2 + 5x + 3$	{32,54,64}	3
6	F_6	$x^3 + 3x^2 + 7x - 2$	{3,32,35}	3
7	F_7	$x^3 - 2x^2 + 5x + 6$	{}	0
8	F_8	$x^3 + 6x^2 + 7x - 1$	{24,55,61}	3
9	F_9	$x^3 - x^2 + 7x + 6$	{32}	1
10	F_{10}	$x^3 + 6x^2 + 5x - 2$	{}	0
11	F_{11}	$x^3 - 2x^2 + 7x + 3$	{}	0
12	F_{12}	$x^3 + 3x^2 + 5x - 4$	{}	0
13	F_{13}	$x^3 - 4x^2 + 3x + 4$	{61}	1
14	F_{14}	$x^3 + 4x^2 + 5x - 3$	{9,19,41}	3
15	F_{15}	$x^3 - 3x^2 + 7x + 2$	{38,41,70}	3
16	F_{16}	$x^3 + 2x^2 + 5x - 6$	{}	0
17	F_{17}	$x^3 - 6x^2 + 7x + 1$	{12,18,49}	3

This completes the proof. □

References

[1] Atkin, A. O. L., Moralin, F., Elliptic Curves and Primality Proving. Math. Comp. 61 (2003)(1993), 29–68.

[2] Buchmann, J., A generalization of Voronoi's unit Algorithm I, II. Journal of Number Theory 20(2) (1985), 177–209.

[3] Buchmann, J., Vollmer, U., Binary Quadratic Forms: An Algorithmic Approach. Berlin, Heidelberg: Springer-Verlag, 2007.

[4] Buell, D. A., Binary Quadratic Forms, Clasical Theory and Modern Computations. New York: Springer-Verlag, 1989.

[5] Delone, B. N., Faddeev, K., The Theory of Irrationalities of the Third Degree. Transl. Math. Monographs 10, Amer. Math. Soc., Providence, Rhode Island 28 (1964), 3955.

[6] Dietmann, R., Small Solutions of Additive Cubic Congruences. Archiv der Mathematik 75 (3)(2000), 195–197.

[7] Flath, D. E., Introduction To Number Theory. Wiley, 1989.

[8] Gezer, B., Özden, H., Tekcan, A., Bizim, O., The Number of Rational Points on Elliptic Curves $y^2 = x^3+b^2$ over Finite Fields. Int. Jour. of Math. Sci. 1(3)(2007), 178-184.

[9] Gezer, B., Tekcan, A., Bizim, O., The Number of Rational Points on Elliptic Curves and Circles over Finite Fields. Inter. Journal of Maths Sciences 2(2)(2008), 58–63.

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

[11] Lenstra, H. W., Jr., Factoring Integers with Elliptic Curves. Ann. of Math. 3(126) (1987), 649–673.

[12] Manin, Y. I., On a Cubic Congrunce to a Prime Modules. Amer. Math. Soc. Transl. 13 (1960), 1–7.

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

[14] Mordell, L. J., On a Cubic Congruence in Three Variables, II. Proc Amer. Math. Soc. 14 (4) (1963), 609–614.

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

[16] Spearman, B. K., Williams, K., The Cubic Congrunce $x^3 + Ax^2 + Bx + C \equiv 0 (\bmod p)$ and Binary Quadratic Forms II. Journal of London Math. Soc. 64 (2) (2001), 273–274.

[17] Voronoi, G. F., On a Generalization of the Algorithm of Continued Fractions, (in Russian). PhD Dissertation, Warsaw, 1896.

[18] Tekcan, A., Bizim, O., The Connection Between Quadratic Forms and the Extended Modular Group. Mathematica Bohemica 128 (3)(2003), 225–236.

[19] Tekcan, A., The Cubic Congruence $x^3 + ax^2 + bx + c \equiv 0 (\bmod p)$ and Binary Quadratic Forms $F(x, y) = ax^2 + bxy + cy^2$. Ars Combinatoria 85(2007), 257–269.

[20] Tekcan, A., On Indefinite Binary Quadratic Forms, Cubic Congruence and Elliptic Curves. Int. Journal of Contemporary Math. Sci 2(21)(2007), 1031-1037.

[21] Tekcan, A., The Number of Rational Points on Conics $C_{p,k} : x^2 - ky^2 = 1$ Over Finite Fields $\mathbb{F}_p$. Int. Jour. of Mathematics Sciences 1 (2) (2007), 150-153.

[22] Tekcan, A., The Elliptic Curves $y^2 = x^3 - t^2x$ over $\mathbb{F}_p$. Int. Jour. of Mathematics Sciences 1(3)(2007), 165-171.

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

[24] Wiles, A., Modular Elliptic Curves and Fermat's Last Theorem. Ann. of Math. 141(3) (1995), 443–551.

[25] Williams, H. C., Zarnke, C. R., Some Algoritms for Solving a Cubic Congruence modulo p. Utilitas Math. 6 (1974), 285–306.

Received by the editors April 9, 2008