International Journal of Engineering, Mathematical and Physical Sciences
ISSN: 2517-9934
Vol:4, No:7, 2010

Positive Definite Quadratic Forms, Elliptic Curves and Cubic Congruences

Ahmet Tekcan

***Abstract*—**Let $F(x,y)=ax^2+bxy+cy^2$ be a positive definite binary quadratic form with discriminant Δ whose base points lie on the line $x=-1/m$ for an integer $m\geq 2$, let p be a prime number and let $\mathbf{F}_p$ be a finite field. Let $E_F: y^2=ax^3+bx^2+cx$ be an elliptic curve over $\mathbf{F}_p$ and let $C_F: ax^3+bx^2+cx\equiv 0(mod\ p)$ be the cubic congruence corresponding to F. In this work we consider some properties of positive definite quadratic forms, elliptic curves and cubic congruences.

***Keywords*—**Binary quadratic form, elliptic curves, cubic congruence.

I. Preliminaries.

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

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

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 $a,b,c\in\mathbf{Z}$, and is positive definite if and only if $\Delta(F)<0$ and $a,c>0$. A positive definite form $F=(a,b,c)$ is said to be reduced if

$$|b|\leq a\leq c. \tag{2}$$

Most properties of quadratic forms can be giving by the aid of extended modular group $\overline{\Gamma}$ (see [20]). Gauss (1777-1855) defined the group action of $\overline{\Gamma}$ on the set of forms as follows:

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

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 $x\rightarrow rx+tu, y\rightarrow sx+uy$. 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 positive definite 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 and if $\det g=-1$, then g is called an improper automorphism. Let $Aut(F)^+$ denote the set of proper automorphisms of F and let $Aut(F)^-$ denote the set of improper automorphisms of F (for further details on binary quadratic forms see [2], [4], [7], [15]).

Ahmet Tekcan is with the Uludag University, Department of Mathematics, Faculty of Science, Bursa-TURKEY, email: tekcan@uludag.edu.tr, http://matematik.uludag.edu.tr/AhmetTekcan.htm.

If a positive definite quadratic form F is not reduced, then we can get it into a reduced form as follows: Let

$$\Omega=\{[1;s;0;1]: s\in\mathbf{Z}\}.$$

Then Ω is a cyclic subgroup of $\mathrm{SL}(2,\mathbf{Z})$ which is generated by $S=[1;1;0;1]$. Now we want to determine the element in the $\Omega-$orbit of F for which the absolute value of xy is minimal. For $s\in\mathbf{Z}$, we have

$$S^sF=(a,b+2sa,as^2+bs+c). \tag{4}$$

Hence the coefficient of x^2 of any form in the $\Omega-$orbit of F is a and the coefficient of xy of such a form is uniquely determined $(mod\ 2a)$. If we choice $s=\left\lfloor\frac{a-b}{2a}\right\rfloor$, then we have $-a<b+2sa\leq a$. This choice of s is minimizes the absolute value of b. Further by (4), the coefficient of y^2 in S^sF is $\frac{(2as+b)^2+|\Delta|}{4a}$, this choice of s minimizes this coefficient. Hence the form $F=(a,b,c)$ is called normal if

$$-a<b\leq a. \tag{5}$$

We see as above that, the $\Omega-$orbit of F contains one normal form which can be obtained as S^sF with $s=\left\lfloor\frac{a-b}{2a}\right\rfloor$. The normal form in the $\Omega-$orbit of F is called the normalization of F, which means replacing F by its normalization. Let $\rho(F)$ denotes the normalization of $(c,-b,a)$. Then ρ is called the reduction operator for positive definite forms. Let $F=F_0=(a_0,b_0,c_0)$ and let

$$s_i=\left\lfloor\frac{b_i+c_i}{2c_i}\right\rfloor. \tag{6}$$

Then by (4), it is easily seen that the reduction of F is

$$\begin{aligned} \rho^{i+1}(F) &= (a_{i+1},b_{i+1},c_{i+1}) \\ &= (c_i,-b_i+2c_is_i,c_is_i^2-b_is_i+a_i) \end{aligned} \tag{7}$$

for $i\geq 0$. If the form $\rho^1(F)$ is not reduced, then we apply the reduction algorithm again and then we find that $\rho^2(F)$. If $\rho^2(F)$ is not reduced, then we apply again and then we find $\rho^3(F)$. So in a finite step $j\geq 1$, we get $\rho^j(F)$ which is reduced. In this case, the form $\rho^j(F)$ is called the reduced type of F.

II. Reduction of Positive Definite Quadratic Forms.

Let $F=(a,b,c)$ be a positive definite quadratic form with discriminant Δ and let $\mathbf{U}=\{z\in\mathbf{C}: Im(z)>0\}$

denote the upper half-plane. Given any positive definite form $F = (a, b, c)$, there exists a unique $z = z(F) \in \mathbf{U}$ such that

$$F = a(x + zy)(x + \overline{z}y). \tag{8}$$

In this case the point z is called the base point of F and is denoted by $z = z(F)$. Let $z = u + iv$. Then (8) becomes

$$\begin{aligned} F = (a, b, c) &= a(x + zy)(x + \overline{z}y) \\ &= ax^2 + 2auxy + a|z|^2y^2. \end{aligned}$$

Hence we find that $u = \frac{b}{2a}$ and $v = \frac{\sqrt{-\Delta}}{2a}$. Note that v is positive. Therefore

$$z = \frac{b + i\sqrt{\Delta}}{2a} \in \mathbf{U}. \tag{9}$$

We may assume that $\mathrm{Im}(z) > 0$ since z and $\overline{z}$ play symmetric roles. So the condition $|b| \leq a$ is equivalent to $|z + \overline{z}| \leq 1$, that is $|Re(z) \leq 1/2|$, and the condition $a \leq c$ is equivalent to $z\overline{z} \geq 1$, that is, $|z| \geq 1$. So the form $F = (a, b, c)$ is reduced if and only if the base point z lies in the fundamental region of $\overline{\Gamma}$, which is the region $\{z \in U : |Re(z)| \leq 1/2, |z| \geq 1\}$.

Conversely for given any point $z \in \mathbf{U}$, there exists a positive definite quadratic form

$$F = (a, b, c) = \left(\frac{1}{|z|^2}, \frac{2u}{|z|^2}, 1\right) \tag{10}$$

of discriminant $\Delta(F) = \frac{-4v^2}{|z|^4}$ whose base point is z. Therefore there is a one-to-one correspondence between positive definite quadratic forms and points in $\mathbf{U}$.

In [20], we considered positive definite quadratic forms $F = (a, b, c)$ whose base points lie on the line $x = -1/m$ for an integer $m \geq 2$. We proved that if m is odd, say $m = 2k+1$, for an integer $k \geq 1$, then there exist $k-$positive definite integral forms of the type

$$F_j = (mj,\ -2j,\ 1), \quad 1 \leq j \leq k$$

of discriminant $\Delta(F_j) = -4j(m-j)$ whose base points $z(F_j)$ lie on the line $x = \frac{-1}{m}$, and if m is even, say $m = 2k$, then there exist $m - 1$ positive definite integral forms of the type

$$F_j = (kj,\ -j,\ 1),\ 1 \leq j \leq m - 1$$

of discriminant $\Delta(F_j) = -j(2m-j)$ whose base points $z(F_j)$ lie on the line $x = \frac{-1}{m}$.

Let

$$F_j^1 = (mj,\ -2j,\ 1),\ 1 \leq j \leq k \tag{11}$$

and

$$F_j^2 = (kj,\ -j,\ 1),\ 1 \leq j \leq m - 1. \tag{12}$$

Note that these forms are not reduced since $c = 1$. But we can get these forms into reduced forms by using the reduction algorithm as we mentioned in the previous section.

Theorem 2.1: If m is odd, then the reduced type of F_j^1 is

$$\rho^1(F_j^1) = (1, 0, mj - j^2) \tag{13}$$

and if m is even, then the reduction type of F_j^2 is

$$\rho^1(F_j^2) = \begin{cases} \left(1, 1, \frac{1-j^2+2mj}{4}\right) & if\ j\ is\ odd \\ \left(1, 1, \frac{-j^2+2mj}{4}\right) & if\ j\ is\ even. \end{cases} \tag{14}$$

Proof: Let $F_j^1 = F_{j_0}^1 = (a_0, b_0, c_0) = (mj,\ -2j,\ 1)$. Then by (6), we get $s_0 = -j$ and hence from (7),

$$\rho^1(F_j^1) = (1, 0, mj - j^2).$$

Note that this form is reduced. Therefore the reduction type of F_j^1 is $\rho^1(F_j^1) = (1, 0, mj - j^2)$.

Similarly let $F_j^2 = F_{j_0}^2 = (a_0, b_0, c_0) = (kj,\ -j,\ 1)$ and let j be odd. Then by (6), we get $s_0 = \frac{1-j}{2}$ and hence

$$\rho^1(F_j^2) = \left(1, 1, \frac{1 - j^2 + 2mj}{4}\right).$$

This form is reduced. Therefore the reduction of F_j^2 is $\rho^1(F_j^2) = \left(1, 1, \frac{1-j^2+2mj}{4}\right)$. Let j be even. Then by (6), we get $s_0 = \frac{-j}{2}$ and hence

$$\rho^1(F_j^2) = \left(1, 0, \frac{-j^2 + 2mj}{4}\right).$$

This form is also reduced. So the reduction of F_j^2 is $\rho^1(F_j^2) = \left(1, 0, \frac{-j^2+2mj}{4}\right)$. This completes the proof. ■

Now we consider the proper and improper automorphisms of F_1^1 and F_j^2 and $\rho^1(F_j^1)$ and $\rho^1(F_j^2)$.

Theorem 2.2: For positive definite forms $F_1^1, F_j^2, \rho^1(F_j^1)$ and $\rho^1(F_j^2)$, we get

$$\begin{aligned} \#Aut(F_j^1)^+ &= \#Aut(F_j^1)^- = 2 \\ \#Aut(F_j^2)^+ &= \#Aut(F_j^2)^- = 2 \end{aligned}$$

and

$$\begin{aligned} \#Aut(\rho^1(F_j^1))^+ &= \#Aut(\rho^1(F_j^1))^- = 2 \\ \#Aut(\rho^1(F_j^2))^+ &= \#Aut(\rho^1(F_j^2))^- = 2 \end{aligned}$$

for every j.

Proof: First we consider the form F_j^1. Recall that an element $g \in \overline{\Gamma}$ is called an automorphism of F if $gF = F$. So we have to find g such that $gF_j^1 = F_j^1$. Let $F_j^1 = (mj,\ -2j,\ 1)$ and let $g = [r; s; t; u] \in \overline{\Gamma}$. Then by (3), we have the following system of equations:

$$\begin{aligned} mjr^2 - 2jrs + s^2 &= mj \\ 2mjrt - 2jru - 2jts + 2su &= -2j \\ mjt^2 - 2jtu + u^2 &= 1. \end{aligned}$$

This system of equations has a solution for $g_1 = \pm[1; 0; 0; 1]$ and $g_2 = \pm[1; 2j; 0; -1]$. Note that $det(g_1) = 1$. So

$$Aut(F_j^1)^+ = \{\pm[1; 0; 0; 1]\}$$

and hence $\#Aut(F_j^1)^+ = 2$ and $det(g_2) = -1$. So

$$Aut(F_j^1)^- = \{\pm[1; 2j; 0; -1]\}$$

and hence $\#Aut(F_j^1)^- = 2$.

For the quadratic form $F_j^2 = (kj, -j, 1)$, the system of equations

$$\begin{aligned} kjr^2 - jrs + s^2 &= kj \\ 2kjrt - jru - jts + 2su &= -j \\ kjt^2 - jtu + u^2 &= 1 \end{aligned}$$

has a solution for $g_1 = \pm[1;0;0;1]$ and $g_2 = \pm[1;j;0;-1]$. Therefore

$$Aut(F_j^2)^+ = \{\pm[1;0;0;1]\}$$

and

$$Aut(F_j^2)^- = \{\pm[1;j;0;-1]\}.$$

So $\#Aut(F_j^2)^+ = \#Aut(F_j^2)^- = 2$.

Similarly it can be show that

$$\#Aut(\rho^1(F_j^1))^+ = \#Aut(\rho^1(F_j^1))^- = 2$$

and

$$\#Aut(\rho^1(F_j^2))^+ = \#Aut(\rho^1(F_j^2))^- = 2.$$

■

III. From Positive Definite Forms to Elliptic Curves.

Mordell began his famous paper (see [16]) 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 (see [10], [13], [14]), for factoring large integers (see [11]), and for primality proving (see [1], [9]). The mathematical theory of elliptic curves was also crucial in the proof of Fermat's Last Theorem (see [30]).

In this section, we want to carry out the results we obtained in the previous section to the singular curves which are the special case of elliptic curves. For this reason, we first give some preliminaries on elliptic curves. An elliptic curve E over a finite field $\mathbf{F}_p$ is defined by an equation in the Weierstrass form

$$E : y^2 = x^3 + ax^2 + bx, \tag{15}$$

where $a, b \in \mathbf{F}_p$ 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 $\mathbf{P}^2$, 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 (x, y) on E

$$E(\mathbf{F}_p) = \{(x, y) \in \mathbf{F}_p \times \mathbf{F}_p : y^2 = x^3 + ax^2 + bx\} \cup \{O\} \tag{16}$$

is a subgroup of E. The order of $E(\mathbf{F}_p)$, denoted by $\#E(\mathbf{F}_p)$, is defined as the number of the points on E and is given by

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

where $(\frac{\cdot}{\mathbf{F}_p})$ denotes the Legendre symbol (for the arithmetic of elliptic curves and rational points on them see [18], [29]).

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

$$E_F : y^2 = ax^3 + bx^2 + cx. \tag{17}$$

If we take $x \to \frac{x}{\sqrt[3]{a}}$ in (17), then we obtain

$$E_F : y^2 = x^3 + ba^{-2/3}x^2 + ca^{-1/3}x. \tag{18}$$

The discriminant of E_F is hence

$$\begin{aligned} \Delta(E_F) &= 16(ca^{-1/3})^2 \left[(ba^{-2/3})^2 - 4(ca^{-1/3}) \right] \\ &= 16(\frac{c}{a})^2 \Delta(F). \end{aligned}$$

So we have a correspondence between binary quadratic forms and elliptic curves, that is, we have the following diagram:

$$\begin{array}{ccc} F & \to & E_F \\ \downarrow & & \downarrow \\ \Delta(F) & \to & \Delta(E_F) = 16(\frac{c}{a})^2 \Delta(F) \end{array}$$

In [8], [23], [24], [25], [26], [27], we considered some specific elliptic curves and derived some results on them. In this section, we consider the same problem for curves corresponding to positive definite forms obtained in Section 2. We proved that if m is odd, $m = 2k + 1$, then there exist $k-$ positive definite integral forms of the type $F_j^1 = (mj, -2j, 1)$ for $1 \leq j \leq k$ of discriminant $\Delta(F_j) = -4j(m - j)$ whose base points $z(F_j)$ lie on the line $x = \frac{-1}{m}$. Now let p be a prime number. Then $F_j^1 = (pj, -2j, 1)$ for $1 \leq j \leq (p - 1)/2$ and let

$$E_{F_j^1} : y^2 = pjx^3 - 2jx^2 + x \tag{19}$$

be the corresponding elliptic curve over $\mathbf{F}_p$. Set

$$E_{F_j^1}(\mathbf{F}_p) = \{(x, y) \in \mathbf{F}_p \times \mathbf{F}_p : y^2 = pjx^3 - 2jx^2 + x\}.$$

Then we have the following theorem.

Theorem 3.1: Let $E_{F_j^1}$ be an elliptic curve defined in (19).

1) If $p \equiv 1, 3 (mod\ 8)$, then

$$\#E_{F_j^1}(F_p) = \begin{cases} p & if\ j \in Q_p \\ p + 2 & if\ j \notin Q_p. \end{cases}$$

2) If $p \equiv 5, 7 (mod\ 8)$, then

$$\#E_{F_j^1}(F_p) = \begin{cases} p & if\ j \notin Q_p \\ p + 2 & if\ j \in Q_p, \end{cases}$$

where Q_p denote the set of quadratic residues.

Proof: (1) Let $p \equiv 1, 3(mod\ 8)$ and let $j \in Q_p$. If $y = 0$, then the cubic congruence has two solutions since

$$\begin{aligned} pjx^3 - 2jx^2 + x \equiv 0(mod\ p) &\Leftrightarrow -2jx^2 + x \equiv 0(mod\ p) \\ &\Leftrightarrow x(1 - 2jx) \equiv 0(mod\ p) \\ &\Leftrightarrow x = 0 \ \ and \ \ x = \frac{1}{2j}. \end{aligned}$$

Let $\frac{1}{2j} \equiv t(mod\ p)$ for some $t \neq 0$. Then there are two rational points $(0, 0)$ and $(t, 0)$ on $E_{F_j^1}$. If $y \neq 0$, then it is easily seen that there are $\frac{p-3}{2}$ integers in $\mathbf{F}_p$ such that $pjx^3 - 2jx^2 + x$ a square. Let $pjx^3 - 2jx^2 + x = u^2$ for some $u \neq 0$. Then $y^2 \equiv u^2(mod\ p) \Leftrightarrow y \equiv \pm u(mod\ p)$. Hence there are two integer solutions, that is, for each point $x \in \mathbf{F}_p$ such that $pjx^3 - 2jx^2 + x$ a square, then there are two rational points (x, u) and $(x, p - u)$ on $E_{F_j^1}$. We know that there are $\frac{p-3}{2}$ integers in $\mathbf{F}_p$ such that $pjx^3 - 2jx^2 + x$ a square. Therefore there are $2\left(\frac{p-3}{2}\right) = p - 3$ rational points on $E_{F_j^1}$. We see as above that there are also two rational points $(0, 0)$ and $(t, 0)$ on $E_{F_j^1}$. Adding the point ∞, we get total $p - 3 + 2 + 1 = p$ rational points on $E_{F_j^1}$.

Now let $j \notin Q_p$. If $y = 0$, then the cubic congruence $pjx^3 - 2jx^2 + x \equiv 0(mod\ p)$ has two solutions since

$$\begin{aligned} pjx^3 - 2jx^2 + x \equiv 0(mod\ p) &\Leftrightarrow -2jx^2 + x \equiv 0(mod\ p) \\ &\Leftrightarrow x(1 - 2jx) \equiv 0(mod\ p) \\ &\Leftrightarrow x = 0 \ \ and \ \ x = \frac{1}{2j}. \end{aligned}$$

Let $\frac{1}{2j} \equiv t(mod\ p)$ for some $t \neq 0$. Then there are two rational points $(0, 0)$ and $(t, 0)$ on $E_{F_j^1}$. Now let $y \neq 0$. Then there are $\frac{p-1}{2}$ integers in $\mathbf{F}_p$ such that $pjx^3 - 2jx^2 + x$ a square. Let $pjx^3 - 2jx^2 + x = u^2$. Then $y^2 \equiv u^2(mod\ p) \Leftrightarrow y \equiv \pm u(mod\ p)$. Hence there are two integer solutions, that is, for each point $x \in \mathbf{F}_p$ such that $pjx^3 - 2jx^2 + x$ a square, then there are two rational points (x, u) and $(x, p - u)$ on $E_{F_j^1}$. We know that there are $\frac{p-1}{2}$ integers in $\mathbf{F}_p$ such that $pjx^3 - 2jx^2 + x$ a square. Therefore there are $2\left(\frac{p-1}{2}\right) = p - 1$ rational points on $E_{F_j^1}$. We know that there are also two rational points $(0, 0)$ and $(t, 0)$ on $E_{F_j^1}$. Adding the point ∞, we get total $p - 1 + 2 + 1 = p + 2$ rational points on $E_{F_j^1}$.

(2) Let $p \equiv 5, 7(mod\ 8)$ and let $j \notin Q_p$. If $y = 0$, then

$$\begin{aligned} pjx^3 - 2jx^2 + x \equiv 0(mod\ p) &\Leftrightarrow -2jx^2 + x \equiv 0(mod\ p) \\ &\Leftrightarrow x(1 - 2jx) \equiv 0(mod\ p) \\ &\Leftrightarrow x = 0 \ \ and \ \ x = \frac{1}{2j}. \end{aligned}$$

Let $\frac{1}{2j} \equiv t(mod\ p)$ for some $t \neq 0$. Then there are two rational points $(0, 0)$ and $(t, 0)$ on $E_{F_j^1}$. Now let $y \neq 0$. Then there are $\frac{p-3}{2}$ integers in $\mathbf{F}_p$ such that $pjx^3 - 2jx^2 + x$ a square. Let $pjx^3 - 2jx^2 + x = u^2$. Then $y^2 \equiv u^2(mod\ p) \Leftrightarrow y \equiv \pm u(mod\ p)$. Hence there are two integer solutions, that is, for each point $x \in \mathbf{F}_p$ such that $pjx^3 - 2jx^2 + x$ a square, then there are two rational points (x, u) and $(x, p - u)$ on $E_{F_j^1}$. We know that there are $\frac{p-3}{2}$ integers in $\mathbf{F}_p$ such that $pjx^3 - 2jx^2 + x$ a square. Therefore there are $2\left(\frac{p-3}{2}\right) = p - 3$ rational points on $E_{F_j^1}$. Adding the points $(0, 0), (t, 0)$ and ∞, we get total $p - 3 + 3 = p$ rational points on $E_{F_j^1}$.

Finally let $j \in Q_p$. If $y = 0$, then

$$\begin{aligned} pjx^3 - 2jx^2 + x \equiv 0(mod\ p) &\Leftrightarrow -2jx^2 + x \equiv 0(mod\ p) \\ &\Leftrightarrow x(1 - 2jx) \equiv 0(mod\ p) \\ &\Leftrightarrow x = 0 \ \ and \ \ x = \frac{1}{2j}. \end{aligned}$$

Let $\frac{1}{2j} \equiv t(mod\ p)$ for some $t \neq 0$. Then there are two rational points $(0, 0)$ and $(t, 0)$ on $E_{F_j^1}$. Now let $y \neq 0$. Then there are $\frac{p-1}{2}$ integers in $\mathbf{F}_p$ such that $pjx^3 - 2jx^2 + x$ a square. Let $pjx^3 - 2jx^2 + x = u^2$. Then $y^2 \equiv u^2(mod\ p) \Leftrightarrow y \equiv \pm u(mod\ p)$. Hence there are two integer solutions, that is, for each point $x \in \mathbf{F}_p$ such that $pjx^3 - 2jx^2 + x$ a square, then there are two rational points (x, u) and $(x, p - u)$ on $E_{F_j^1}$. We know that there are $\frac{p-1}{2}$ integers in $\mathbf{F}_p$ such that $pjx^3 - 2jx^2 + x$ a square. Therefore there are $2\left(\frac{p-1}{2}\right) = p - 1$ rational points on $E_{F_j^1}$. Adding the points $(0, 0), (t, 0)$ and ∞, we get total $p - 1 + 3 = p + 2$ rational points on $E_{F_j^1}$. ■

Remark 3.2: Note that we only consider the number of rational points on elliptic curves $E_{F_j^1}$ and $E_{\rho^1(F_j^1)}$ corresponding the forms F_j^1 and its reduced type $\rho^1(F_j^1)$, respectively. When we consider the quadratic forms F_j^2 and its reduced type $\rho^1(F_j^2)$ and so elliptic curves $E_{F_j^2}$ and $E_{\rho^1(F_j^2)}$, then we find that there is no rule for the number of rational points on them since m is even.

IV. From Positive Definite Forms to Cubic Congruences.

In 1896, Voronoi (see [28]) presented his algorithm for computing a system of fundamental units of a cubic number field. His technique, described in terms of binary quadratic forms. Later his technique was restarted in the language of multiplicative lattices by Delone and Faddeev (see [5]). In 1985, Buchmann (see [3]) generalized the Voronoi's algorithm. Recall that a cubic congruence over a field $\mathbf{F}_p$ is

$$x^3 + ax^2 + bx + c \equiv 0(mod\ p), \tag{20}$$

where $a, b, c \in \mathbf{F}_p$ and p is prime. Solutions of cubic congruence (including cubic residues) was considered by many authors. Dietmann (see [6]) considered the small solutions of additive cubic congruences. Manin (see [12]) considered the cubic congruence on prime modules. Mordell (see [17]) considered the cubic congruence in three variables and also the congruence $ax^3 + by^3 + cz^3 + dxyz \equiv n(mod\ p)$. Williams and Zarnke (see [31]) 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 $\mathbf{Q}(\sqrt{\Delta})$, 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 [19], Spearman and Williams considered the cubic congruence $x^3 + ax^2 + bx + c \equiv 0(mod\ p)$ and binary

quadratic forms $F(x,y) = ax^2 + bxy + cy^2$. They proved that the cubic congruence $x^3 + ax^2 + bx + c \equiv 0(mod\ p)$ 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 [21], [22], we considered the number of integer solutions of cubic congruences $ax^3 + bx^2 + cx \equiv 0(mod\ p)$ for an indefinite binary quadratic form $F(x,y) = ax^2 + bxy + cy^2$. In this section, we consider the same problem for positive definite forms F_j^1. Let p be a prime number. Then $F_j^1 = (pj, -2j, 1)$ and hence the cubic congruence associated with F_j^1 is

$$C_{F_j^1} : pjx^3 - 2jx^2 + x \equiv 0(mod\ p). \tag{21}$$

Let $C_{F_j^1}(\mathbf{F}_p) = \{x \in \mathbf{F}_p : pjx^3 - 2jx^2 + x \equiv 0(mod\ p)\}$. Then we have the following theorem.

Theorem 4.1: Let $C_{F_j^1}$ be a cubic congruence defined in (21). Then

$$\#C_{F_j^1}(\mathbf{F}_p) = 2$$

for all primes $p \geq 5$.

Proof: For the cubic congruence, $C_{F_j^1}$, we have

$$\begin{aligned} & pjx^3 - 2jx^2 + x \equiv 0(mod\ p) \\ \Leftrightarrow\ & -2jx^2 + x \equiv 0(mod\ p) \\ \Leftrightarrow\ & x(-2jx + 1) \equiv 0(mod\ p) \\ \Leftrightarrow\ & x = 0 \ \ and \ \ x = \frac{1}{2j}, \end{aligned}$$

that is, there are two solutions of $C_{F_j^1}$. So $\#C_{F_j^1}(\mathbf{F}_p) = 2$. ■

Now we consider the cubic congruence associated with the reduced type of F_j^1. Recall that the reduction of F_j^1 is $\rho^1(F_j^1) = (1, 0, pj - j^2)$ by (13). So the associated cubic congruence is

$$C_{\rho^1(F_j^1)} : x^3 + (pj - j^2)x \equiv 0(mod\ p). \tag{22}$$

Let $C_{\rho^1(F_j^1)}(\mathbf{F}_p) = \{x \in \mathbf{F}_p : x^3 + (pj - j^2)x \equiv 0(mod\ p)\}$. Then we have the following theorem.

Theorem 4.2: Let $C_{\rho^1(F_j^1)}$ be a cubic congruence defined in (22). Then

$$\#C_{\rho^1(F_j^1)}(\mathbf{F}_p) = 3$$

for all primes $p \geq 5$.

Proof: For the cubic congruence $C_{\rho^1(F_j^1)}$, we have

$$\begin{aligned} & x^3 + (pj - j^2)x \equiv 0(mod\ p) \\ \Leftrightarrow\ & x^3 - j^2x \equiv 0(mod\ p) \\ \Leftrightarrow\ & x(x^2 - j^2) \equiv 0(mod\ p) \\ \Leftrightarrow\ & x(x - j)(x + j) \equiv 0(mod\ p) \\ \Leftrightarrow\ & x = 0,\ x = j \ \ and \ \ x = p - j. \end{aligned}$$

So $\#C_{\rho^1(F_j^1)}(\mathbf{F}_p) = 3$. ■

REFERENCES

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

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

[3] J. Buchmann. *A generalization of Voronoi's unit algorithm I,II.* J. Number Theory **20**(1985), 177–191, 192–209.

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

[5] B.N. Delone and D.K. Faddeev. *The Theory of Irrationalities of the Third Degree.* Transl. Math. Monographs 10, Amer. Math. Soc., Providence, Rhode Island 1964.

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

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

[8] B. Gezer, H.Özden, A.Tekcan, O.Bizim. *The Number of Rational Points on Elliptic Curves $y^2 = x^3 + b^2$ over Finite Fields*. International Journal of Computational and Mathematical Sciences **1**(3)(2007), 178–184.

[9] 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.

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

[11] H.W.Jr. Lenstra. *Factoring Integers with Elliptic Curves.* Annals of Maths. **126**(2)(1987), 649–673.

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

[13] 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.

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

[15] R.A. Mollin. *Advanced Number Theory with Applications*. CRC Press, Taylor and Francis Group, Boca Raton, London, New York, 2009.

[16] 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.

[17] L.J. Mordell. *On the Congruence $ax^3 + by^3 + cz^3 + dxyz \equiv n(mod\ p)$.* Duke Math. J. **31**(1)(1964), 123–126.

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

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

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

[21] 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.

[22] A. Tekcan. *The Cubic Congruence $x^3 + ax^2 + bx + c \equiv 0(mod\, p)$ and Binary Quadratic Forms $F(x,y) = ax^2 + bxy + cy^2$ II.* Accepted for publication to Acta Universitatis Apulensis.

[23] A .Tekcan. *The Elliptic Curves $y^2 = x^3 - t^2x$ over F_p.* International Journal of Comp. and Maths. Sci. **1**(3)(2007), 165–171.

[24] A. Tekcan, A. Özkoç, B. Gezer, O. Bizim. *Elliptic Curves, Conics and Cubic Congruencies associated with Indefinite Binary Quadratic Forms*. Novi Sad Journal of Mathematics **38**(2)(2008), 71–81.

[25] A. Tekcan. *The Number of Rational Points on Singular Curves $y^2 = x(x-a)^2$ over Finite Fields F_p.* Int. Journal of Comp.and Math.Sci. **3**(1)(2009), 14–17.

[26] A. Tekcan. *The Elliptic Curves $y^2 = x^3 - 1728x$ over Finite Fields*. Journal of Algebra, Number Theory: Advances and Applications **1**(1)(2009), 61–74.

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

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

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

[30] A. Wiles. *Modular Elliptic Curves and Fermat's Last Theorem.* Annals of Maths. **141**(3)(1995), 443–551.

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