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 \( \Delta \) whose base points lie on the line \( x = -1/m \) for an integer \( m \geq 2 \), let \( p \) be a prime number and let \( \mathbb{F}_p \) be a finite field. Let \( E_F : y^2 = ax^2 + bxy + cy^2 \) be an elliptic curve over \( \mathbb{F}_p \) and let \( C_F : ax^2 + bxy + cy^2 \equiv 0 \pmod{p} \) 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

\[
F = F(x, y) = ax^2 + bxy + cy^2
\]

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 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

\[
|b| \leq a \leq c.
\]

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

\[
gF(x, y) = (ax^2 + brs + cs^2)x^2 + (2art + bru + bts + 2csu)xy + (a^2 + btu + cu^2)y^2
\]

for \( g = \left( \begin{array}{cc} r & s \\ t & u \end{array} \right) \in \Gamma \), that is, \( gF \) is gotten from \( F \) by making the substitution \( x = rx + tu, y = sx + uy \).

Moreover, \( \Delta(F) = \Delta(gF) \) for all \( g \in \Gamma \), that is, the action of \( \Gamma \) on forms leaves the discriminant invariant. If \( F \) is positive definite or integral, then so is \( gF \) for all \( g \in \Gamma \). Let \( F \) and \( G \) be two forms. If there exists a \( g \in \Gamma \) 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.

The set of improper automorphisms of \( F \) (for further details on binary quadratic forms see [2], [4], [7], [15]).

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

\[
\Omega = \{(1; s; 0; 1) : s \in \mathbb{Z} \}.
\]

Then \( \Omega \) is a cyclic subgroup of \( SL(2, \mathbb{Z}) \) 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 \( s \in \mathbb{Z} \), we have

\[
S^sF = (a, b + 2as, as^2 + bs + c).
\]

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 \( (\bmod 2a) \). If we choose \( s = \frac{a+b}{2a} \), then we have \( -a < b + 2sa \leq a \). This choice of \( s \) 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

\[
-a < b \leq a.
\]

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

\[
s_i = \left[ \frac{b_i + c_i}{2c_i} \right].
\]

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

\[
\rho^{i+1}(F) = (a_{i+1}, b_{i+1}, c_{i+1}) = (c_i - b_i + 2c_i s_i, c_i s_i^2 - b_i s_i + a_i)
\]

for \( i \geq 0 \). If the form \( \rho^i(F) \) 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 \( \Delta \) and let \( U = \{z \in \mathbb{C} : Im(z) > 0 \} \)
denote the upper half-plane. Given any positive definite form \( F = (a, b, c) \), there exists a unique \( z = z(F) \in \mathbb{U} \) such that
\[
F = a(x + zy)(x + \overline{z}y).
\]
(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
\[
F = a(x + zy)(x + \overline{z}y) = ax^2 + 2auxy + a|z|^2y^2.
\]

Hence we find that \( u = \frac{b}{2a} \) and \( v = \frac{\sqrt{-\Delta}}{2a} \). Note that \( v \) is positive. Therefore
\[
z = \frac{b + i\sqrt{-\Delta}}{2a} \in \mathbb{U}.
\]
(9)

We may assume that \( \text{Im}(z) > 0 \) since \( z \) and \( \overline{z} \) play symmetric roles. So the condition \( |b| \leq a \) is equivalent to \( |z + \overline{z}| \leq 1 \), that is \( |Re(z) - \frac{1}{2}| \leq 1 \), and the condition \( a \leq c \) is equivalent to \( \Delta \geq 1 \), 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 domain of \( \Gamma \), which is the region \( \{ z \in \mathbb{U} : |Re(z)| ≤ \frac{1}{2}, |z| ≥ 1 \} \).

Conversely for given any point \( z \in \mathbb{U} \), there exists a positive definite quadratic form
\[
F = (a, b, c) = \left( \frac{1}{|z|^2}, \frac{2u}{|z|^2}, 1 \right)
\]
(10)
of discriminant \( \Delta(F) = \frac{4c^2}{|z|^4} \) whose base point is \( z \). Therefore there is a one-to-one correspondence between positive definite quadratic forms and points in \( \mathbb{U} \).

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
\[
F_j = (kj, -j, 1), \quad 1 \leq j \leq m-1
\]
of discriminant \( \Delta(F_j) = -j(2m-j) \) whose base points \( z(F_j) \) lie on the line \( x = \frac{-1}{m} \).

Let
\[
F_j = (mj, -2j, 1), \quad 1 \leq j \leq k
\]
(11)
and
\[
F_j = (kj, -j, 1), \quad 1 \leq j \leq m-1.
\]
(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 \( F_j \) is
\[
\rho^1(F_j) = (1, 0, mj - j^2)
\]
(13)
and if \( m \) is even, then the reduction type of \( F_j \) is
\[
\rho^1(F_j) = \begin{cases} (1, 1, \frac{1-j^2+2mj}{4}) & \text{if } j \text{ is odd} \\ (1, 1, \frac{-j^2+2mj}{4}) & \text{if } j \text{ is even.} \end{cases}
\]
(14)

**Proof**: Let \( F_1 = F_{j_0} = (a_0, b_0, c_0) = (mj, -2j, 1) \). Then by (6), we get \( s_0 = -j \) and hence from (7),
\[
\rho^1(F_1) = (1, 0, mj - j^2).
\]
Note that this form is reduced. Therefore the reduction type of \( F_1 \) is \( \rho^1(F_1) = (1,0,mj - j^2) \).

Similarly let \( F_j = F_{j_0} = (a_0, b_0, c_0) = (kj, -j, 1) \) and let \( j \) be odd. Then by (6), we get \( s_0 = \frac{-j}{2} \) and hence
\[
\rho^1(F_j) = \left( 1, 1, \frac{1-j^2+2mj}{4} \right).
\]
This form is reduced. Therefore the reduction of \( F_j \) is \( \rho^1(F_j) = \left( 1, 1, \frac{1-j^2+2mj}{4} \right) \).

Let \( j \) be even. Then by (6), we get \( s_0 = \frac{-j}{2} \) and hence
\[
\rho^1(F_j) = \left( 1, 0, \frac{-j^2+2mj}{4} \right).
\]
This form is also reduced. So the reduction of \( F_j \) is \( \rho^1(F_j) = \left( 1, 0, \frac{-j^2+2mj}{4} \right) \). This completes the proof.

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

**Theorem 2.2**: For positive definite forms \( F_1, F_j, \rho^1(F_1) \) and \( \rho^1(F_j) \), we get
\[
#\text{Aut}(F_1) = 2
\]
\[
#\text{Aut}(F_2) = 2
\]
and
\[
#\text{Aut}(\rho^1(F_1)) = 2
\]
\[
#\text{Aut}(\rho^1(F_2)) = 2
\]
for every \( j \).

**Proof**: First we consider the form \( F_1 \). Recall that an element \( g \in \Gamma \) is called an automorphism of \( F \) if \( gF = F \). So we have to find \( g \) such that \( gF_1 = F_1 \). Let \( F_1 = (mj, -2j, 1) \) and let \( g = [r,s,t,u] \in \Gamma \). Then by (3), we have the following system of equations:
\[
jmjr^2 - 2jrs + s^2 = mj
\]
\[
2mjr - 2jru - 2jts + 2su = -2j
\]
\[
jmjt^2 - 2jtu + u^2 = 1.
\]
This system of equations has a solution for \( q_1 = \pm [1; 0; 0; 1] \) and \( q_2 = \pm [1; 2j; 0; -1] \). Note that \( \text{det}(q_1) = 1 \). So
\[
\text{Aut}(F_1) = \{ \pm [1; 0; 0; 1] \}
\]
and hence \( \#\text{Aut}(F_1) = 2 \) and \( \text{det}(q_2) = -1 \). So
\[
\text{Aut}(F_1) = \{ \pm [1; 2j; 0; -1] \}
\]
and hence \( \#\text{Aut}(F_j^2)^- = 2 \).

For the quadratic form \( F_j^2 = (kj, -j, 1) \), the system of equations
\[
\begin{align*}
kjr^2 - jrs + s^2 &= kj \\
kjrte - jsu + ts + 2su &= -j \\
kjt^2 - jtu + u^2 &= 1
\end{align*}
\]
has a solution for \( g_1 = \pm[1; 0; 0; 1] \) and \( g_2 = \pm[1; j; 0; -1] \).

Therefore
\[
\text{Aut}(F_j^2)^+ = \{ \pm[1; 0; 0; 1] \}
\]
and
\[
\text{Aut}(F_j^2)^- = \{ \pm[1; j; 0; -1] \}.
\]

So \( \#\text{Aut}(F_j^2)^+ = \#\text{Aut}(F_j^2)^- = 2 \).

Similarly it can be shown that
\[
\#\text{Aut}(\rho^1(F_j^2)) = \#\text{Aut}(\rho^1(F_j^2))^- = 2
\]
and
\[
\#\text{Aut}(\rho^1(F_j^2))^+ = \#\text{Aut}(\rho^1(F_j^2))^- = 2.
\]

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
\[
E : y^2 = x^3 + ax^2 + bx,
\]
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 \( \Delta(E) = 0 \), the curve 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
\[
y^2z = x^3 + ax^2z + bxz^3
\]
and one point at infinity, namely \((0, 1, 0)\). This point \( \infty \) is the point where all vertical lines meet. We denote this point by \( O \). The set of rational points \((x, y)\) on \( E \)
\[
E(\mathbf{F}_p) = \{(x, y) \in \mathbf{F}_p \times \mathbf{F}_p : y^2 = x^3 + ax^2 + bx^3\} \cup \{O\}
\]
is a subgroup of \( E \). The order of \( E(\mathbf{F}_p) \), denoted by \( \#\text{E}(\mathbf{F}_p) \), is defined as the number of the points on \( E \) and is given by
\[
\#\text{E}(\mathbf{F}_p) = p + 1 + \sum_{x \in \mathbf{F}_p} \left( \frac{x^3 + ax^2 + bx}{\mathbf{F}_p} \right),
\]
where \( \left( \frac{\cdot}{\mathbf{F}_p} \right) \) 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
\[
E_F : y^2 = ax^3 + bx^2 + cx.
\]
If we take \( x \to \frac{x}{\sqrt{n}} \) in (17), then we obtain
\[
E_F : y^2 = x^3 + ba^{-2/3}x^2 + ca^{-1/3}x.
\]
The discriminant of \( E_F \) is hence
\[
\Delta(E_F) = 16(ca^{-1/3} - 2)(ba^{-2/3})^2 - 4(\xi^{-1/3})^2
\]
\[
= 16(\xi^{-1/3})^2 \Delta(F).
\]

So we have a correspondence between binary quadratic forms and elliptic curves, that is, we have the following diagram:
\[
\begin{array}{ccc}
F & \rightarrow & E_F \\
\downarrow & & \downarrow \\
\Delta(F) & \rightarrow & \Delta(E_F) = 16(\xi^{-1/3})^2 \Delta(F)
\end{array}
\]

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 \( F_j^1 = \langle m, j \rangle - 2j \), \( 1 \leq j \leq k \) of discriminant \( \Delta(F_j^1) = -4(\xi - m) \) where base points \( z(F_j^1) \) lie on the line \( x = \frac{1}{4}m \). Now let \( p \) be a prime number. Then \( F_j^1 = \langle p, j \rangle - 2j \), \( 1 \leq j \leq \frac{p - 1}{2} \) and let
\[
E_{F_j^1} : y^2 = pju^3 - 2ju^2 + x.
\]
be the corresponding elliptic curve over \( \mathbf{F}_p \). Set
\[
E_{F_j^1}(\mathbf{F}_p) = \{(x, y) \in \mathbf{F}_p \times \mathbf{F}_p : y^2 = pju^3 - 2ju^2 + x\}.
\]

Then we have the following theorem.

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

1) If \( p \equiv 1, 3 \text{ (mod 8)} \), then

\[
\#E_{F_j^1}(\mathbf{F}_p) = \begin{cases} 
p & \text{if } j \in Q_p \\
p + 2 & \text{if } j \notin Q_p. \end{cases}
\]

2) If \( p \equiv 5, 7 \text{ (mod 8)} \), then

\[
\#E_{F_j^1}(\mathbf{F}_p) = \begin{cases} 
p & \text{if } j \notin Q_p \\
p + 2 & \text{if } j \in Q_p, \end{cases}
\]

where \( Q_p \) denote the set of quadratic residues.
Proof: (1) Let \( p \equiv 1, 3 \, (\text{mod} \, 8) \) and let \( j \in \mathbb{Q}_p \). If \( y = 0 \), then the cubic congruence has two solutions since
\[
p jx^3 - 2jx^2 + x \equiv 0 \, (\text{mod} \, p) \quad \iff \quad -2jx^2 + x \equiv 0 \, (\text{mod} \, p)
\]
\[
x = 1 - 2jx \equiv 0 \, (\text{mod} \, p)
\]
\[
x = 0 \quad \text{and} \quad x = \frac{1}{2j}.
\]
Let \( \frac{1}{2j} \equiv t \, (\text{mod} \, p) \) for some \( t \neq 0 \). Then there are two rational points \((0, 0)\) and \((t, 0)\) on \( E_{F_j} \). If \( y \neq 0 \), then it is easily seen that there are \( \frac{p-3}{2} \) integers in \( F_p \) such that \( pjx^3 - 2jx^2 + x \) a square. Let \( pjx^3 - 2jx^2 + x = u^2 \) for some \( u \neq 0 \). Then \( y^2 \equiv u^2 \, (\text{mod} \, p) \) \( \Rightarrow y \equiv \pm u \, (\text{mod} \, p) \). Hence there are two integer solutions, that is, for each point \( x \in F_p \), such that \( pjx^3 - 2jx^2 + x \) a square, then there are two rational points \((x, u)\) and \((x, p - u)\) on \( E_{F_j} \). We know that there are \( \frac{p-3}{2} \) integers in \( F_p \) such that \( pjx^3 - 2jx^2 + x \) a square. Therefore there are \( 2 \left( \frac{p-3}{2} \right) = p - 3 \) rational points on \( E_{F_j} \).

Now let \( j \notin \mathbb{Q}_p \). If \( y = 0 \), then the cubic congruence \( pjx^3 - 2jx^2 + x \equiv 0 \, (\text{mod} \, p) \) has two solutions since
\[
p jx^3 - 2jx^2 + x \equiv 0 \, (\text{mod} \, p) \quad \iff \quad -2jx^2 + x \equiv 0 \, (\text{mod} \, p)
\]
\[
x = 1 - 2jx \equiv 0 \, (\text{mod} \, p)
\]
\[
x = 0 \quad \text{and} \quad x = \frac{1}{2j}.
\]
Let \( \frac{1}{2j} \equiv t \, (\text{mod} \, p) \) for some \( t \neq 0 \). Then there are two rational points \((0, 0)\) and \((t, 0)\) on \( E_{F_j} \). Now let \( y \neq 0 \). Then there are \( \frac{p-3}{2} \) integers in \( F_p \) such that \( pjx^3 - 2jx^2 + x \) a square. Let \( pjx^3 - 2jx^2 + x = u^2 \). Then \( y^2 \equiv u^2 \, (\text{mod} \, p) \) \( \Rightarrow y \equiv \pm u \, (\text{mod} \, p) \). Hence there are two integer solutions, that is, for each point \( x \in F_p \), such that \( pjx^3 - 2jx^2 + x \) a square, then there are two rational points \((x, u)\) and \((x, p - u)\) on \( E_{F_j} \). We know that there are \( \frac{p-3}{2} \) integers in \( F_p \) such that \( pjx^3 - 2jx^2 + x \) a square. Therefore there are \( 2 \left( \frac{p-3}{2} \right) = p - 1 \) rational points on \( E_{F_j} \). Adding the points \((0, 0), (t, 0)\) and \( \infty \), we get total \( p + 1 = p + 2 \) rational points on \( E_{F_j} \).

Remark 3.2: Note that we only consider the number of rational points on elliptic curves \( E_{F_j} \) and \( E_{F_j}(F_j) \) corresponding the forms \( F_j \) and its reduced type \( \rho^j(F_j) \), respectively. When we consider the quadratic forms \( F_j^2 \) and its reduced type \( \rho^j(F_j) \) and so elliptic curves \( E_{F_j} \) and \( E_{F_j}(F_j) \), 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 1986, Voronoï (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 Voronoï’s algorithm. Recall that a cubic congruence over a field \( F_p \) is
\[
x^3 + ax^2 + bx + c \equiv 0 \, (\text{mod} \, p),
\]
where \( a, b, c \in F_p \) 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 \( ax^3 + by^3 + cz^3 + dxyz \equiv n \, (\text{mod} \, p) \). 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 \( \Delta \). 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 [19], 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 $x^3 + ax^2 + bx + c \equiv 0 \pmod{p}$ has three solutions if and only if it is represented by a quadratic form $F$ in $J$, where $J = J(L, K, F_1)$ is a subgroup of index 3 in $H(\Delta(K)/f_1^2)$.\\n
In [21], [22], we considered the number of integer solutions of cubic congruences $ax^3 + bx^2 + cx \equiv 0 \pmod{p}$ 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 $C_{F_j} : pjx^3 - 2jx^2 + x \equiv 0 \pmod{p}$. (21)\\n
Let $C_{F_j}(F_p) = \{ x \in F_p : pjx^3 - 2jx^2 + x \equiv 0 \pmod{p} \}$. Then we have the following theorem.

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

$$\#C_{F_j}(F_p) = 2$$

for all primes $p \geq 5$.

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

$$\begin{align*}
&pjx^3 - 2jx^2 + x \equiv 0 \pmod{p} \\
\iff &-2jx^2 + x \equiv 0 \pmod{p} \\
\iff &x(-2jx + 1) \equiv 0 \pmod{p} \\
\iff &x = 0 \text{ and } x = \frac{1}{2j}.
\end{align*}$$

that is, there are two solutions of $C_{F_j}$. So $\#C_{F_j}(F_p) = 2$.

Now we consider the cubic congruence associated with the reduced type of $F_1^1$. Recall that the reduction of $F_1^1$ is $\rho^1(F_1^1) = (1, 0, pj - j^2)$ by (13). So the associated cubic congruence is $C_{\rho^1(F_1)} : x^3 + (pj - j^2)x \equiv 0 \pmod{p}$. (22)\\n
Let $C_{\rho^1(F_1)}(F_p) = \{ x \in F_p : x^3 + (pj - j^2)x \equiv 0 \pmod{p} \}$. Then we have the following theorem.

**Theorem 4.2:** Let $C_{\rho^1(F_1)}$ be a cubic congruence defined in (22). Then

$$\#C_{\rho^1(F_1)}(F_p) = 3$$

for all primes $p \geq 5$.

Proof: For the cubic congruence $C_{\rho^1(F_1)}$, we have

$$\begin{align*}
&x^3 + (pj - j^2)x \equiv 0 \pmod{p} \\
\iff &x^3 - j^2x \equiv 0 \pmod{p} \\
\iff &x(x^2 - j^2) \equiv 0 \pmod{p} \\
\iff &x(x - j)(x + j) \equiv 0 \pmod{p} \\
\iff &x = 0, x = j \text{ and } x = p - j.
\end{align*}$$

So $\#C_{\rho^1(F_1)}(F_p) = 3$.\n
**REFERENCES**


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

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


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


