C. R. Math. Rep. Acad. Sci. Canada Vol. **31** (2) 2009, pp. 53–64

POSITIVE DEFINITE BINARY QUADRATIC FORMS, QUADRATIC CONGRUENCES, AND SINGULAR CURVES

AHMET TEKCAN AND ARZU ÖZKOÇ

Presented by Edward Bierstone, FRSC

ABSTRACT. We consider some properties of positive definite binary quadratic forms F_j in the family Ω. We determine the number of integer solutions of quadratic congruences C_{F_j} and determine the number of rational points on singular curves E_{F_j} related to F_j over finite fields $\mathbb{F}_p$.

RÉSUMÉ. On considère quelques propriétés des formes quadratiques binaires définies positives F_j dans la famille Ω. On détermine le nombre de solutions entières des congruences quadratiques C_{F_j}, et le nombre de points rationnels sur des courbes singulières E_{F_j} reliées aux F_j sur des corps finis $\mathbb{F}_p$.

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 $\Delta = \Delta(F)$. Moreover, 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 form $F = (a, b, c)$ is called *primitive* if $\gcd(a, b, c) = 1$. 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 the extended modular group $\overline{\Gamma}$ (see [8]). Gauss [3] defined the group action of $\overline{\Gamma}$ on the set of forms as

$$gF(x, y) = (ar^2 + brs + cs^2)x^2 + (2art + bru + bts + 2csu)xy + (at^2 + btu + cu^2)y^2$$

for $g = \left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right) = [r; s; t; u] \in \overline{\Gamma}$. 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*. Since equivalence provides us with equivalence classes, then there is a means of composing or multiplying these classes to get a group. The notation of composition of forms, as given in Gauss [3] is much

Received by the editors on August 20, 2008.
AMS Subject Classification: Primary: 11E04 secondary: 11E16, 11D09, 11D79, 11G07, 11G20, 14G05.
Keywords: binary quadratic form, elliptic curve, singular curve, quadratic congruence.

longer and more difficult than the method of Dirichlet [1]. Moreover, Dirichlet's method provides a clearer link with the ideal theory [5]. If $F_1 = (a_1, b_1, c_1)$ and $F_2 = (a_2, b_2, c_2)$ are two forms of discriminant Δ, then they are called *united* if $\gcd(a_1, a_2, \frac{b_1+b_2}{2}) = 1$. So if F_1 and F_2 are two united forms, then there exists a unique integer K modulo $2a_1a_2$ such that $B \equiv b_i (\mathrm{mod}\ 2a_i)$ for $i = 1, 2$ and also $B^2 \equiv \Delta (\mathrm{mod}\ 4a_1a_2)$. The form composed of strictly primitive united forms F_1 and F_2 is $F_1 o F_2 = (a_1a_2, B, C)$, where B is defined as above and $C = \frac{B^2-\Delta}{4a_1a_2}$. Under composition, the classes of strictly primitive forms of discriminant Δ form a finite abelian group C^1_Δ whose order h^1_Δ is the number of classes of equivalent, strictly primitive forms, called the *class number* of the form class group C^1_Δ (see also [2]).

Mollin, in his book [5], considered the arithmetic of ideals. Let $D \neq 1$ be a square-free integer and let $\Delta = \frac{4D}{r^2}$, where $r = 2$ if $D \equiv 1 (\mathrm{mod}\ 4)$ and $r = 1$, otherwise. If we set $\mathbb{K} = \mathbb{Q}(\sqrt{D})$, then $\mathbb{K}$ is called a quadratic number field of discriminant Δ. Thus there is a one-to-one correspondence between quadratic fields and square-free rational integers $D \neq 1$. A complex number is an *algebraic integer* if it is the root of a monic polynomial with coefficients in $\mathbb{Z}$. The set of all algebraic integers in the complex field $\mathbb{C}$ is a ring which we denote by A. Then $A \cap \mathbb{K} = O_\Delta$ is the ring of integers of the quadratic field $\mathbb{K}$ of discriminant Δ. Let $I = [\alpha, \beta]$ denote the $\mathbb{Z}$-module $\alpha\mathbb{Z} \oplus \beta\mathbb{Z}$ for $\alpha, \beta \in \mathbb{K}$, *i.e.,* the additive abelian group, with basis elements α and β consisting of $\{\alpha x + \beta y : x, y \in \mathbb{Z}\}$. Then $O_\Delta = \left[1, \frac{1+\sqrt{D}}{r}\right]$. In this case $w_\Delta = \frac{r-1+\sqrt{D}}{r}$ is called the *principal surd*. Every principal surd $w_\Delta \in O_\Delta$ can be uniquely expressed as $w_\Delta = x\alpha + y\beta$, where $x, y \in \mathbb{Z}$ and $\alpha, \beta \in O_\Delta$. We call α, β an *integral basis* for $\mathbb{K}$. If $\frac{\alpha\overline{\beta}-\beta\overline{\alpha}}{\sqrt{\Delta}} > 0$, then α and β are called *ordered basis elements*. Two bases of an ideal are ordered if and only if they are equivalent under an element of $\overline{\Gamma}$. If I has ordered basis elements, then we say that I is simply ordered. If I is ordered, then

$$F(x, y) = \frac{N(\alpha x + \beta y)}{N(I)}$$

is a quadratic form of discriminant Δ (here $N(x)$ denote the norm of x). In this case we say that F belongs to I and write $I \to F$. Conversely let us assume that

$$G(x, y) = Ax^2 + Bxy + Cy^2 = d(ax^2 + bxy + cy^2)$$

is a quadratic form, where $d = \pm \gcd(A, B, C)$ and $b^2 - 4ac = \Delta$. If $B^2 - 4AC > 0$, then we get $d > 0$ and if $B^2 - 4AC < 0$, then we choose d such that $a > 0$. If

$$I = [\alpha, \beta] = \begin{cases} \left[a, \dfrac{b-\sqrt{\Delta}}{2}\right] & \text{for } a > 0, \\ \left[a, \dfrac{b-\sqrt{\Delta}}{2}\right]\sqrt{\Delta} & \text{for } a < 0 \text{ and } \Delta > 0, \end{cases}$$

then I is an ordered O_Δ-ideal. Note that if $a > 0$, then I is primitive and if $a < 0$, then $\frac{I}{\sqrt{\Delta}}$ is primitive. Thus to every form G, there corresponds an ideal

I to which G belongs and we write $G \to I$. Hence we have a correspondence between ideals and quadratic forms.

Let δ denote a real quadratic irrational integer with trace $t = \delta + \overline{\delta}$ and norm $n = \delta\overline{\delta}$. Given a real quadratic irrational $\gamma \in \mathbb{Q}(\delta)$, there are rational integers P and Q such that $\gamma = \frac{P+\delta}{Q}$ with $Q|(\delta+P)(\overline{\delta}+P)$. Hence for each $\gamma = \frac{P+\delta}{Q}$, there is a corresponding $\mathbb{Z}$-module $I_\gamma = [Q,\ P+\delta]$ (in fact, this module is an ideal) and an indefinite quadratic form $F_\gamma(x,y) = Q(x+\gamma y)(x+\overline{\gamma}y)$ of discriminant $\Delta = t^2 - 4n$. The ideal I_γ is said to be *reduced* if and only if $P+\delta > Q$ and $-Q < P + \overline{\delta} < 0$ and is said to be *ambiguous* if and only if it contains both $\frac{P+\delta}{Q}$ and $\frac{P+\overline{\delta}}{Q}$ so if and only if $\frac{2P}{Q} \in \mathbb{Z}$. Let $[m_0; \overline{m_1, m_2, \ldots, m_{l-1}}]$ denote the continued fraction expansion of γ with period length $l = l(I)$, where

$$m_i = \Big\lfloor \frac{P_i + \delta}{Q_i} \Big\rfloor, \quad P_{i+1} = m_i Q_i - P_i, \quad \text{and} \quad Q_{i+1} = \frac{\delta^2 - P_{i+1}^2}{Q_i}, \quad \text{for } i \geq 0.$$

From the continued fraction factoring algorithm we get all reduced ideals equivalent to a given reduced ideal I_γ, *i.e.,* in the continued fraction expansion of γ we have $I_\gamma = I_\gamma^0 \sim I_\gamma^1 \sim \cdots \sim I_\gamma^{l-1}$. Finally $I_\gamma^l = I_\gamma^0$ for a complete cycle of reduced ideals of length $l(I) = l$. Two O_Δ-ideals I and J are called *narrowly* (or *strictly*) *equivalent* if they satisfy the property $(\alpha)I = (\beta)J$ for some $\alpha, \beta \in O_\Delta$ with $N(\alpha\beta) > 0$. In this case, we write $I \approx J$.

2. **Positive definite binary quadratic forms.** Let p be a prime number such that $p \geq 5$, and let

$$F_j = (a_j, b_j, c_j) = \Big(1, 2j, \frac{p-1}{2}j\Big) \tag{2.1}$$

be a binary quadratic form of discriminant $\Delta = 4j^2 - 2j(p-1)$ for $1 \leq j \leq \frac{p-1}{2}$. Set

$$\Omega = \Big\{F_j : F_j = \Big(1, 2j, \frac{p-1}{2}j\Big), 1 \leq j \leq \frac{p-1}{2}\Big\}.$$

In this section, we consider some properties of F_j in Ω. First we consider the reduction of F_j. Note that F_j is not reduced, since $|b_j| > a_j$. It is known that if a positive definite form $F = (a,b,c)$ is not reduced, then it can be transformed into a reduced form by using the reduction algorithm defined as follows: let $F = F_0 = (a_0, b_0, c_0)$ and let

$$s_i = \Big\lfloor \frac{b_i + c_i}{2c_i} \Big\rfloor. \tag{2.2}$$

Then the reduction of F is

$$\rho^{i+1}(F) = (a_{i+1}, b_{i+1}, c_{i+1}) = (c_i, -b_i + 2c_i s_i, c_i s_i^2 - b_i s_i + a_i) \tag{2.3}$$

for $i \geq 0$. If the form $\rho^1(F)$ is not reduced, then we apply the reduction algorithm again and we find that $\rho^2(F)$. If $\rho^2(F)$ is not reduced, then we apply again and 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.

THEOREM 2.1. *Let F_j be the positive definite form in Ω. Then the reduced type of F_j is*

$$\rho^2(F_j) = \begin{cases} (1,0,1) & \text{if } p = 5, \\ \left(1, 0, -j^2 + \frac{p-1}{2}j\right) & \text{if } p > 5, \end{cases} \tag{2.4}$$

for $1 \leq j \leq \frac{p-3}{2}$.

PROOF. Let $p = 5$. Then $F_1 = (1,2,2)$. Let $F_0 = F_{1_0} = (a_0, b_0, c_0) = (1,2,2)$. Then by (2.2), we get $s_0 = 1$ and hence $\rho^1(F_1) = (a_1, b_1, c_1) = (2,2,1)$ by (2.3). But this form is not reduced since $|b_1| > c_1$. If we apply the reduction algorithm again, then we get $s_1 = 1$ and hence $\rho^2(F_1) = (a_2, b_2, c_2) = (1,0,1)$. It is easily seen that the form $\rho^2(F_1)$ is reduced. So the reduced type of F_1 is $\rho^2(F_1) = (1,0,1)$.

Now let $p > 5$. Since $p > 5$, we can write $\frac{2j + j\frac{(p-1)}{2}}{j(p-1)} < 1$ for $F_j = \left(1, 2j, \frac{p-1}{2}j\right)$. So

$$s_0 = \left\lfloor \frac{b_0 + c_0}{2c_0} \right\rfloor = \left\lfloor \frac{2j + \frac{p-1}{2}j}{(p-1)j} \right\rfloor = 0$$

and hence $\rho^1(F_j) = (a_1, b_1, c_1) = \left(\frac{p-1}{2}j, -2j, 1\right)$. But this form is not reduced since $|b_1| > c_1$. If we apply the reduction algorithm again, then we get $s_1 = -j$ and hence $\rho^2(F_j) = (a_2, b_2, c_2) = \left(1, 0, -j^2 + \frac{p-1}{2}j\right)$. It is easily seen that the form $\rho^2(F_j)$ is reduced. So the reduced type of F_j is $\rho^2(F_j) = \left(1, 0, -j^2 + \frac{p-1}{2}j\right)$. □

Now we consider the proper and improper automorphisms of F_j and their reduced type $\rho^2(F_j)$. Recall that 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 $\mathrm{Aut}(F)^+$ denote the set of proper automorphisms of F and let $\mathrm{Aut}(F)^-$ denote the set of improper automorphisms of F. Then we can give the following theorem.

THEOREM 2.2. *Let F_j and $\rho^2(F_j)$ be two forms defined in* (2.1) *and* (2.4)*, respectively. Then*

$$\#\,\mathrm{Aut}(F_j)^+ = \#\,\mathrm{Aut}(F_j)^- = \#\,\mathrm{Aut}(\rho^2(F_j))^+ = \mathrm{Aut}(\rho^2(F_j))^- = \begin{cases} 4 & \text{if } p = 5, \\ 2 & \text{if } p > 5, \end{cases}$$

for every j such that $1 \leq j \leq \frac{p-3}{2}$.

PROOF. Let $p = 5$. Then $F_1 = (1, 2, 2)$. Let $g = [r; s; t; u] \in \overline{\Gamma}$. Then the system of equations

$$r^2 + 2rs + 2s^2 = 1, \quad 2rt + 2ru + 2ts + 4su = 2,$$
$$t^2 + 2tu + 2u^2 = 2.$$

has a solution for $g = \pm[1; 0; 0; 1], \pm[1; -1; 2; -1]$. So

$$\mathrm{Aut}(F_1)^+ = \{\pm[1; 0; 0; 1], \pm[1; -1; 2; -1]\}.$$

Similarly $\mathrm{Aut}(F_1)^- = \{\pm[1; -1; 0; -1], \pm[1; 0; 2; -1]\}$. If $p > 5$, then

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

With the same argument we find that for $p = 5$

$$\mathrm{Aut}(\rho^2(F_1))^+ = \{\pm[1; 0; 0; 1], \pm[0; -1; 1; 0]\},$$
$$\mathrm{Aut}(\rho^2(F_1))^- = \{\pm[1; 0; 0; -1], \pm[0; 1; 1; 0]\}$$

and for $p > 5$

$$\mathrm{Aut}(\rho^2(F_j))^+ = \{\pm[1; 0; 0; 1]\},$$
$$\mathrm{Aut}(\rho^2(F_j))^- = \{\pm[1; 0; 0; -1]\}.$$

This completes the proof. □

REMARK 1. In Theorem 2.2 we only considered the forms F_j and $\rho^2(F_j)$ for $1 \le j \le \frac{p-3}{2}$. Note that the forms $F_{(p-1)/2}$ and $\rho^2(F_{(p-1)/2})$ have discriminants $\Delta = 0$. So they are not positive definite. Nevertheless in this case,

$$\#\,\mathrm{Aut}(F_{\frac{p-1}{2}})^+ = \#\,\mathrm{Aut}(F_{\frac{p-1}{2}})^- = \#\,\mathrm{Aut}(\rho^2(F_{\frac{p-1}{2}}))^+$$
$$= \#\,\mathrm{Aut}(\rho^2(F_{\frac{p-1}{2}}))^- = \infty$$

for every prime $p \ge 5$.

Now we can prove that the form F_j and $\rho^2(F_j)$ are ambiguous for every $1 \le j \le \frac{p-1}{2}$. We see in Section 1 that there is a correspondence between ideals and quadratic forms. We see that strictly primitive ideals correspond to strictly primitive forms. Also strictly reduced forms correspond to strictly reduced ideals. Note that two strictly reduced forms $F_1 = (a_1, b_1, c_1)$ and $F_2 = (a_2, b_2, c_2)$ are called *adjacent* if $b_1 + b_2 \equiv 0 (\mathrm{mod}\ 2a_1)$. Since the number of strictly reduced forms is finite for a given discriminant Δ and adjacent forms are equivalent via the transformation $g = [0; -1; 1; \frac{b_1+b_2}{2a_1}]$, the list of successively adjacent forms

must return the original form, and they are all equivalent. In fact, two strictly reduced forms are equivalent if and only if they are in the same cycle as described above and the number of forms in a given cycle (called the period of the cycle) is always even. So a quadratic form F of type $F = (a, ka, c)$ for some $k \in \mathbb{Z}$ is called *ambiguous*. In other words, a form F is called ambiguous if it is improperly equivalent to itself, that is, there exists an element $g \in \overline{\Gamma}$ with $\det g = -1$ such that $gF = F$. In this case, the class of F is called an ambiguous class.

Now we can give the following theorem.

THEOREM 2.3. *The forms F_j and $\rho^2(F_j)$ are ambiguous for every $1 \leq j \leq \frac{p-1}{2}$.*

PROOF. We see as above that the set of improper automorphisms of F_j and $\rho^2(F_j)$ is non-empty, that is, there exists at least one element $g_1 \in \mathrm{Aut}(F_j)^-$ and $g_2 \in \mathrm{Aut}(\rho^2(F_j))^-$ with $\det g_1 = \det g_2 = -1$ such that $g_1 F_j = F_j$ and $g_2 \rho^2(F_j) = \rho^2(F_j)$. So F_j and $\rho^2(F_j)$ are ambiguous. □

3. **Quadratic congruences related to F_j.** Let $F = (a, b, c)$ be a binary quadratic form and let C_F: $ax^2 + bxy + cy^2 \equiv 1 (\mathrm{mod}\ p)$ be the corresponding quadratic congruence over finite fields $\mathbb{F}_p$. In this section, we consider the number of integer solutions of quadratic congruences related to F_j and $\rho^2(F_j)$. But we only consider the forms F_1 and $F_{(p-1)/2}$ and so $\rho^2(F_1)$ and $\rho^2(F_{(p-1)/2})$. Let

$$C_{F_1} : x^2 + 2xy + \frac{p-1}{2}y^2 \equiv 1 \pmod{p}, \tag{3.1}$$

$$C_{F_{\frac{p-1}{2}}} : x^2 + (p-1)xy + \left(\frac{p-1}{2}\right)^2 y^2 \equiv 1 \pmod{p}, \tag{3.2}$$

$$C_{\rho^2(F_1)} : x^2 + \frac{p-3}{2}y^2 \equiv 1 \pmod{p}, \tag{3.3}$$

$$C_{\rho^2(F_{\frac{p-1}{2}})} : x^2 \equiv 1 \pmod{p}, \tag{3.4}$$

be the corresponding quadratic congruences, respectively and let

$$C_{F_1}(\mathbb{F}_p) = \left\{(x, y) \in \mathbb{F}_p \times \mathbb{F}_p : x^2 + 2xy + \frac{p-1}{2}y^2 \equiv 1 \pmod{p}\right\},$$

$$C_{F_{\frac{p-1}{2}}}(\mathbb{F}_p) = \left\{(x, y) \in \mathbb{F}_p \times \mathbb{F}_p : x^2 + (p-1)xy + \left(\frac{p-1}{2}\right)^2 y^2 \equiv 1 \pmod{p}\right\},$$

$$C_{\rho^2(F_1)}(\mathbb{F}_p) = \left\{(x, y) \in \mathbb{F}_p \times \mathbb{F}_p : x^2 + \frac{p-3}{2}y^2 \equiv 1 \pmod{p}\right\},$$

$$C_{\rho^2(F_{\frac{p-1}{2}})}(\mathbb{F}_p) = \{(x, y) \in \mathbb{F}_p \times \mathbb{F}_p : x^2 \equiv 1 \pmod{p}\}.$$

Then we have the following theorem.

THEOREM 3.1. *Let C_{F_1}, $C_{F_{(p-1)/2}}$, $C_{\rho^2(F_1)}$ and $C_{\rho^2(F_{(p-1)/2})}$ be the quadratic congruences defined in* (3.1), (3.2), (3.3), *and* (3.4), *respectively. Then*

$$\#C_{F_{\frac{p-1}{2}}}(\mathbb{F}_p) = \#C_{\rho^2(F_{\frac{p-1}{2}})}(\mathbb{F}_p) = 2p$$

for every prime $p \geq 5$, and

$$\#C_{F_1}(\mathbb{F}_p) = \#C_{\rho^2(F_1)}(\mathbb{F}_p) = \begin{cases} p-1 & \text{if } p \equiv 1,5,19,23 \pmod{24}, \\ p+1 & \text{if } p \equiv 7,11,13,17 \pmod{24}. \end{cases}$$

PROOF. We first consider the quadratic congruence $C_{F_{(p-1)/2}}$. If $y = 0$, then $x^2 \equiv 1 \pmod{p} \Leftrightarrow x \equiv \pm 1 \pmod{p}$. If $x = 0$, then

$$\Big(\frac{p-1}{2}\Big)^2 y^2 \equiv 1 \pmod{p} \Leftrightarrow y \equiv \pm 2 \pmod{p}$$

since $\big(\frac{p-1}{2}\big)^2(\pm 2)^2 = p^2 - 2p + 1 \equiv 1 \pmod{p}$. Further $(1,4)$ and $(p-1, p-4)$ are also solutions of $C_{F_{(p-1)/2}}$ since $1^2 + (p-1)\cdot 1 \cdot 4 + \big(\frac{p-1}{2}\big)^2 \cdot 4^2 = 4p^2 - 4p + 1 \equiv 1 \pmod{p}$ and

$$(p-1)^2 + (p-1)(p-1)(p-4) + \Big(\frac{p-1}{2}\Big)^2 (p-4)^2 = \frac{p^4}{4} - \frac{3p^3}{2} + \frac{13p^2}{4} - 3p + 1 \equiv 1 \pmod{p}.$$

So we have six integer solutions $(1,0)$, $(p-1,0)$, $(0,2)$, $(0,p-2)$, $(1,4)$, and $(p-1,p-4)$ of (3.2).

Let $H_p = \mathbb{F}_p - \{0, 1, p-1\}$. Note that $p^2 - 2p + 1 \equiv 1 \pmod{p}$ and also $(p-1)^2 \mid 2((1-p)x \pm 1)$. Now we want to solve the quadratic congruence according to y, where x is taken in H_p. Applying (3.2), we find that

$$\Big(\frac{p-1}{2}\Big)^2 y^2 + (p-1)xy + x^2 - 1 = 0. \tag{3.5}$$

The discriminant of (3.5) is

$$\Delta = ((p-1)x)^2 - 4\Big(\frac{p-1}{2}\Big)^2 (x^2 - 1) = p^2 - 2p + 1 \equiv 1 \pmod{p}.$$

Hence the solutions of (3.5) are

$$y_{1,2} = \frac{-(p-1)x \pm \sqrt{p^2 - 2p + 1}}{2\big(\frac{p-1}{2}\big)^2} \equiv \frac{2[-(p-1)x \pm 1]}{(p-1)^2} \pmod{p}.$$

We know that $(p-1)^2 | 2((1-p)x \pm 1)$. So there are two integer solutions y, that is, for every $x \in H_p$, there are two solutions $y \in \mathbb{F}_p^*$. We know that there are $p-3$ elements $x \in H_p$. Consequently, there are $2(p-3) = 2p-6$ solutions y. Adding the integer solutions $(1,0)$, $(p-1,0)$, $(0,2)$, $(0,p-2)$, $(1,4)$, and $(p-1,p-4)$, we find that there are a total of $2p - 6 + 6 = 2p$ integer solutions, that is, $\#C_{F_{(p-1)/2}}(\mathbb{F}_p) = 2p$. The others are similar. □

4. **Singular curves related to F_j.** In this section, we will consider the number of rational points on singular curves related to quadratic forms F_j defined in (2.1). Singular curves are in fact a special case of elliptic curves. Before starting our problem, we give some notations on elliptic curves. Let q be a positive integer and let $\mathbb{F}_q$ be a finite field and let $\overline{\mathbb{F}}_q$ denote the algebraic closure of $\mathbb{F}_q$ with $\mathrm{char}(\overline{\mathbb{F}}_q) \neq 2, 3$. An elliptic curve E over $\mathbb{F}_q$ is defined by an equation

$$E : y^2 = x^3 + ax^2 + bx,$$

where $a, b \in \mathbb{F}_q$ and $b^2(a^2 - 4b) \neq 0$. If $b^2(a^2 - 4b) = 0$, then E is called *singular*. 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 (x, y) on E

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

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

$$\#E(\mathbb{F}_q) = q + 1 + \sum_{x \in \mathbb{F}_q} \Big(\frac{x^3 + ax^2 + bx}{\mathbb{F}_q}\Big),$$

where $(\frac{\cdot}{\mathbb{F}_q})$ denotes the Legendre symbol (for further details on the arithmetic of elliptic curves, see [6, 9]).

Now we can return to our problem. Let $E_{F_j} : y^2 = x^3 + 2jx^2 + \frac{p-1}{2}jx$ be the corresponding curve for $1 \leq j \leq \frac{p-1}{2}$. Note that if $1 \leq j \leq \frac{p-3}{2}$, then E_{F_j} is an elliptic curve and if $j = \frac{p-1}{2}$, then $E_{F_{(p-1)/2}}$ is a singular curve. Let

$$E_{F_{\frac{p-1}{2}}} : y^2 = x^3 + (p-1)x^2 + \frac{(p-1)^2}{4}x \tag{4.1}$$

and let

$$E_{F_{\frac{p-1}{2}}}(\mathbb{F}_p) = \Big\{(x, y) \in \mathbb{F}_p \times \mathbb{F}_p : y^2 = x^3 + (p-1)x^2 + \frac{(p-1)^2}{4}x\Big\} \cup \{O\}.$$

In [4, 7], we considered the number of rational points on elliptic curves $y^2 = x^3 + b^2$ and $y^2 = x^3 - t^2x$ over $\mathbb{F}_p$, respectively. In this section, we consider the same problem for singular curves $E_{F_{(p-1)/2}}$ defined in (4.1).

THEOREM 4.1. *Let $E_{F_{(p-1)/2}}$ be the singular curve defined in* (4.1). *Then*

$$\#E_{F_{\frac{p-1}{2}}}(\mathbb{F}_p) = \begin{cases} p & \text{if } p \equiv 1, 7 \pmod 8, \\ p + 2 & \text{if } p \equiv 3, 5 \pmod 8. \end{cases}$$

PROOF. Recall that $E_{F_{(p-1)/2}} : y^2 = x^3 + (p-1)x^2 + \frac{(p-1)^2}{4}x$. Now let $p \equiv 1, 7 \pmod 8$. If $y = 0$, then we get

$$
\begin{aligned}
(4.2) \qquad & x^3 + (p-1)x^2 + \Big(\frac{p-1}{2}\Big)^2 x \equiv 0 \pmod p \\
& \Leftrightarrow x\Big[x^2 + (p-1)x + \Big(\frac{p-1}{2}\Big)^2\Big] \equiv 0 \pmod p \\
& \Leftrightarrow x \equiv 0 \pmod p \text{ and } x^2 + (p-1)x + \Big(\frac{p-1}{2}\Big)^2 \equiv 0 \pmod p.
\end{aligned}
$$

Hence, it is easily seen that $x = 0$ and $x = \frac{p+1}{2}$ are the solutions of (4.2). So we have two rational points $(0,0)$ and $(\frac{p+1}{2}, 0)$ on $E_{F_{(p-1)/2}}$. Further, it is easily seen that if $p \equiv 1, 7 (\mathrm{mod}\, 8)$, then $\frac{p+1}{2} \in Q_p$ (the set of quadratic residues). Let x be a quadratic residue mod p, that is, $(\frac{x}{p}) = 1$. Then we get

$$\Big(\frac{x^3 + (p-1)x^2 + \Big(\frac{p-1}{2}\Big)^2 x}{p}\Big) = \Big(\frac{x - \frac{p+1}{2}}{p}\Big).$$

So if $x = \frac{p+1}{2}$, then $\big(\frac{x-\frac{p+1}{2}}{p}\big) = 0$. Hence the quadratic congruence $y^2 \equiv 0 \pmod p$ has one solution $y = 0$ as we mentioned above. If $x \neq \frac{p+1}{2}$, then $\big(\frac{x-\frac{p+1}{2}}{p}\big) = 1$, that is, $x^3 + (p-1)x^2 + \big(\frac{p-1}{2}\big)^2 x$ is a square mod p. Let

$$x^3 + (p-1)x^2 + \Big(\frac{p-1}{2}\Big)^2 x = u^2$$

for $u \in \mathbb{F}_p^* = \mathbb{F}_p - \{0\}$. Then $y^2 \equiv u^2 \pmod p \Leftrightarrow y \equiv \pm u \pmod p$. Hence there are two points (x, u) and $(x, p-u)$ on $E_{F_{(p-1)/2}}$, that is, for every x, there are two points. We know that there are $\frac{p-1}{2} - 1 = \frac{p-3}{2}$ (we subtract 1 from the number of quadratic residues since $x = \frac{p+1}{2}$ is a quadratic residue but for this value of x, there is one solution y. For the other values of x, there are two solutions y) elements x such that $x^3 + (p-1)x^2 + \big(\frac{p-1}{2}\big)^2 x$ a square. Hence there are $2\big(\frac{p-3}{2}\big) = p - 3$ points on $E_{F_{(p-1)/2}}$. We see as above that there are two points $(0,0)$ and $\big(\frac{p+1}{2}, 0\big)$ on $E_{F_{(p-1)/2}}$. Adding the point ∞, we get a total $3 - p + 2 + 1 = p$ points on $E_{F_{(p-1)/2}}$.

The other assertion is similar. □

REMARK 2. (i) Note that in the above theorem we only consider the number of rational points on singular curves. We know that E_{F_j} is an elliptic curve for $1 \leq j \leq \frac{p-3}{2}$. But for these values of j, we cannot determine the number of rational points on E_{F_j}.

(ii) If $p \equiv 1,7 \pmod 8$ or $p \equiv 3,5 \pmod 8$, then

$$\Big(\frac{x^3+(p-1)x^2+\left(\frac{p-1}{2}\right)^2 x}{p}\Big) = -1$$

for every $x \notin Q_p$. So there is no rational point on $E_{(p-1)/2}$.

EXAMPLE 1. Let $p = 23$. Then the rational points on $E_{F_{11}} : y^2 = x^3 + 22x^2 + 6x$ over $\mathbb{F}_{23}$ are

$$E_{F_{11}}(\mathbb{F}_{23}) = \left\{ \begin{array}{c} (\mathbf{0},\mathbf{0}), (1,\pm 11), (2,\pm 4), (3,\pm 6), (4,\pm 7), (6,\pm 3), (8,\pm 6), \\ (9,\pm 9), (\mathbf{12},\mathbf{0}), (13,\pm 6), (16,\pm 7), (18,\pm 2) \end{array} \right\} \cup \{O\}.$$

EXAMPLE 2. Let $p = 37$. Then the rational points on $E_{F_{18}} : y^2 = x^3 + 36x^2 + 28x$ over $\mathbb{F}_{37}$ are

$$E_{F_{18}}(\mathbb{F}_{37}) = \left\{ \begin{array}{l} (\mathbf{0},\mathbf{0}),\ (1,\pm 18),\ (3,\pm 18),\ (4,\pm 7),\ (7,\pm 3),\ (9,\pm 7), \\ (10,\pm 12),\ (11,\pm 1),\ (12,\pm 12),\ (16,\pm 12),\ (\mathbf{19},\mathbf{0}), \\ (21,\pm 11),\ (25,\pm 7),\ (26,\pm 4),\ (27,\pm 10),\ (28,\pm 14), \\ (30,\pm 2),\ (33,\pm 17),\ (34,\pm 18),\ (36,\pm 9) \end{array} \right\} \cup \{O\}.$$

Let $[x]$ and $[y]$ denote the x- and y-coordinates of the points (x, y) on $E_{F_{(p-1)/2}}$, respectively. Then we have the following results.

THEOREM 4.2. *The sum of* $[x]$ *on* $E_{F_{(p-1)/2}}$ *is*

$$\sum_{[x]} E_{F_{\frac{p-1}{2}}}(\mathbb{F}_p) = \begin{cases} \dfrac{p^3-7p-6}{12} & \text{if } p \equiv 1,7 \pmod 8, \\ \dfrac{p^3+5p+6}{12} & \text{if } p \equiv 3,5 \pmod 8. \end{cases}$$

PROOF. Let $U_p = \{1, 2, \ldots, p-1\}$ 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. Then the sum of all elements in Q_p is $\sum_{x\in Q_p} x = \frac{p^3-p}{24}$.

Let $p \equiv 1,7 \pmod 8$. Then we know that $\frac{p+1}{2} \in Q_p$. But for this value of x there is one point $\left(\frac{p+1}{2}, 0\right)$ on $E_{F_{(p-1)/2}}$. Now let $H_p = Q_p - \left\{\frac{p+1}{2}\right\}$. Then

$$\sum_{x\in H_p} x = \sum_{x\in Q_p} x - \frac{p+1}{2} = \frac{p^3-13p-12}{24}.$$

We also know that every element x in H_p makes $x^3 + (p-1)x^2 + \left(\frac{p-1}{2}\right)^2 x$ a square. Let $x^3 + (p-1)x^2 + \left(\frac{p-1}{2}\right)^2 x = t^2$. Then $y^2 \equiv t^2 \pmod p$. 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 $x \in H_p$, 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 $E_{F_{(p-1)/2}}$ is $2\sum_{x\in H_p} x$. Furthermore, as we said above, the point $\left(\frac{p+1}{2},0\right)$ is also on $E_{F_{(p-1)/2}}$. So

$$\sum_{[x]} E_{F_{\frac{p-1}{2}}}(\mathbb{F}_p) = \frac{p+1}{2} + 2\sum_{x\in H_p} x = \frac{p^3-7p-6}{12}.$$

Similarly it can be shown that if $p \equiv 3,5 \pmod 8$, then

$$\sum_{[x]} E_{F_{\frac{p-1}{2}}}(\mathbb{F}_p) = \frac{p^3+5p+6}{12}.$$

□

THEOREM 4.3. *The sum of* $[y]$ *on* $E_{F_{(p-1)/2}}$ *is*

$$\sum_{[y]} E_{F_{\frac{p-1}{2}}}(\mathbb{F}_p) = \begin{cases} \frac{p^2-3p}{2} & \text{if } p \equiv 1,7 \pmod 8, \\ \frac{p^2-p}{2} & \text{if } p \equiv 3,5 \pmod 8. \end{cases}$$

PROOF. Let $p \equiv 1,7 \mod 8$. Then we know by Theorem 4.1 that there are $\frac{p-3}{2}$ points x such that $x^3+(p-1)x^2+\left(\frac{p-1}{2}\right)^2 x$ a square, that is,

$$\left(\frac{x^3+(p-1)x^2+\left(\frac{p-1}{2}\right)^2 x}{\mathbb{F}_p}\right) = 1.$$

Let $x^3+(p-1)x^2+\left(\frac{p-1}{2}\right)^2 x = t^2$ for some integer $t \neq 0$. Then the quadratic congruence $y^2 \equiv t^2 \pmod p \Leftrightarrow y \equiv \pm t \pmod p$ 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 in H_p such that $x^3+(p-1)x^2+\left(\frac{p-1}{2}\right)^2 x$ is a square. So

$$\sum_{[y]} E_{F_{\frac{p-1}{2}}}(\mathbb{F}_p) = p\left(\frac{p-3}{2}\right) = \frac{p^2-3p}{2}.$$

Similarly it can be shown that if $p \equiv 3,5 \pmod 8$, then,

$$\sum_{[y]} E_{F_{\frac{p-1}{2}}}(\mathbb{F}_p) = \frac{p^2-p}{2}.$$

□

References

1. D. A. Buell, *Binary Quadratic Forms, Clasical Theory and Modern Computations.* Springer-Verlag, New York, 1989.
2. D. E. Flath, *Introduction to Number Theory.* Wiley, New, York, 1989.
3. C. F. Gauss, *Disquisitiones Arithmeticae.* Springer-Verlag, New York, 1986.
4. 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. J. Math. Sci. **1** (2007), no. 3, 178–184.
5. R. A. Mollin, *Quadratics.* CRC Press, Boca Raton, FL, 1996.
6. J. H. Silverman, *The Arithmetic of Elliptic Curves.* Graduate Texts in Mathematics 106. Springer-Verlag, New York, 1986.
7. A. Tekcan *The elliptic curves $y^2 = x^3 - t^2x$ over $\mathbb{F}_p$.* Int. J. Math. Sci.**1** (2007), no. 3, 165–171.
8. A. Tekcan and O. Bizim, *The connection between quadratic forms and the extended modular group.* Math. Bohem. **128** (2003), no. 3, 225–236.
9. L. C. Washington, *Elliptic Curves. Number Theory and Cryptography.* CRC, Boca Raton, FL, 2003.

Department of Mathematics
Faculty of Science
Uludag University
Görükle, Bursa
Türkiye
email: *tekcan@uludag.edu.tr*
aozkoc@uludag.edu.tr