n-UNIVERSAL QUADRATIC FORMS, QUADRATIC IDEALS AND ELLIPTIC CURVES OVER FINITE FIELDS

AHMET TEKCAN and ARZU ÖZKOÇ

In this work, we derive some properties of n-universal quadratic forms, quadratic ideals and elliptic curves over finite fields $\mathbb{F}_p$ for primes $p \geq 5$. In the first section, we give some preliminaries form binary quadratic forms and quadratic idelas. In the second section, we consider the quadratic ideals and quadratic forms. In the third section, we consider the quadratic forms over finite fields, also consider the representations of positive integers by quadratic forms and n-universal forms. In the last section, we consider the number of rational points on elliptic curves associated with the universal forms.

AMS 2010 Subject Classification: 11E04, 11E16, 11E18, 14G05.

Key words: quadratic irrationals, quadratic ideals, indefinite quadratic forms, universal form, elliptic curve.

1. **PRELIMINARIES**

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

$$F = F(x, y) = ax^2 + bxy + cy^2 \tag{1.1}$$

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

$$\left|\sqrt{\Delta} - 2|a|\right| < b < \sqrt{\Delta} \tag{1.2}$$

(for further details on binary quadratic forms see [1, 2, 5, 9, 10]). Most properties of quadratic forms can be giving by the aid of extended modular group $\overline{\Gamma}$ (see [12]). Gauss (1777–1855) defined the group action of $\overline{\Gamma}$ on the set of forms as follows

$$gF(x,y) = \tag{1.3}$$
$$= \left(ar^2+brs+cs^2\right)x^2+(2art+bru+bts+2csu)\,xy+\left(at^2+btu+cu^2\right)y^2$$

for $g=\begin{pmatrix} r & s \\ t & u \end{pmatrix}=[r;s;t;u]\in\overline{\Gamma}$. Moreover, $\Delta(F)=\Delta(gF)$ for all $g\in\overline{\Gamma}$, that is, the action of $\overline{\Gamma}$ on forms leaves the discriminant invariant. If F is indefinite or integral, then so is gF for all $g\in\overline{\Gamma}$. Let F and G be two forms. If there exists a $g\in\overline{\Gamma}$ such that $gF=G$, then F and G are called equivalent. If $\det g=1$, then F and G are called properly equivalent, and if $\det g=-1$, then F and G are called improperly equivalent. A quadratic form F is called ambiguous if it is improperly equivalent to itself. An element $g\in\overline{\Gamma}$ is called an automorphism of F if $gF=F$. If $\det g=1$, then g is called a proper automorphism of F, and if $\det g=-1$, then g is called an improper automorphism of F. Let $\mathrm{Aut}(F)^+$ denote the set of proper automorphisms of F and let $\mathrm{Aut}(F)^-$ denote the set of improper automorphisms of F.

Mollin [9] considered the arithmetic of ideals in his book. Let $D\neq 1$ be a square free integer and let $\Delta=\frac{4D}{r^2}$, where $r=2$ if $D\equiv 1(\bmod 4)$ 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 and O_Δ is the ring of integers of the quadratic field $\mathbb{K}$ of discriminant Δ. Let $I=[\alpha,\beta]$ denote the $\mathbb{Z}$-module $\alpha\mathbb{Z}\oplus\beta\mathbb{Z}$, i.e., the additive abelian group, with basis elements α and β consisting of $\{\alpha x+\beta y : x,y\in\mathbb{Z}\}$. Note that $O_\Delta=\left[1,\frac{1+\sqrt{D}}{r}\right]$. 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 $[\alpha,\beta]$ 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. Recall that two basis 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 $N(x)$ denotes the norm of x). In this case we say that F belongs to I and write $I\to F$. Conversely, let us assume that $G(x,y)=Ax^2+Bxy+Cy^2=d(ax^2+bxy+cy^2)$ be 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 $I=[\alpha,\beta]=\left[a,\frac{b-\sqrt{\Delta}}{2}\right]$ for $a>0$ or $\left[a,\frac{b-\sqrt{\Delta}}{2}\right]\sqrt{\Delta}$ for $a<0$ and $\Delta>0$, 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 (for further details see [1, 9]).

Theorem 1.1. *Let $I = [a,\, b + cw_\Delta]$. Then I is a non-zero ideal of O_Δ if and only if $c|b$, $c|a$ and $ac|N(b + cw_\Delta)$* ([9]).

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

$$I_\gamma = [Q,\, P + \delta] \tag{1.4}$$

(in fact, this module is an ideal by Theorem 1.1), and an indefinite quadratic form

$$F_\gamma(x, y) = Q(x + \delta y)(x + \overline{\delta} y) \tag{1.5}$$

of discriminant $\Delta = t^2 - 4n$. The ideal I_γ in (1.4) 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 $\frac{2P}{Q} \in \mathbb{Z}$.

2. QUADRATIC IDEALS AND QUADRATIC FORMS

In this section, we will consider some properties of quadratic ideals and indefinite quadratic forms. First we give the following definition (see [3, 4]).

Definition 2.1. Let n be any integer. If there exists a $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ such that

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

then n can be represented by F. If a form F represents all integers, then it called universal.

Let $F(x, y) = x^2 + 5xy + 6y^2$ be an indefinite binary quadratic form. Then F is universal. Indeed for any integer n, the quadratic equation $F(x, y) = x^2 + 5xy + 6y^2 = n$ has a solution for $(x, y) = (2 - 3n, n - 1)$. Since F is universal every prime number p can be also represented by F. Let $P = 2 - 3p$, $Q = p - 1$ and $D = P^2 + 5PQ + 6Q^2 = p$. Then $\gamma = \frac{P+\sqrt{D}}{Q}$ is a quadratic irrational and hence

$$I_\gamma = [p - 1, 2 - 3p + \sqrt{p}] \tag{2.1}$$

is a quadratic ideal and

$$F_\gamma = (p - 1, 4 - 6p, 9p - 4) \tag{2.2}$$

is an indefinite binary quadratic form of discriminant $\Delta = 4p$. Then we can give the following two theorems.

Theorem 2.2. *The ideal I_γ in* (2.1) *is not reduced and is not ambiguous for any prime $p \geq 5$.*

Proof. Note that $|2-3p| > p-1$ and also $16p^2-25p+9>0$ since $p \geq 5$. So, we have

$$\begin{aligned} 16p^2-25p+9>0 &\Leftrightarrow 16p^2-24p+9>p \Leftrightarrow 4p-3>\sqrt{p} \\ &\Leftrightarrow p-1>(2+3p)+\sqrt{p} \Leftrightarrow Q>P+\sqrt{D}. \end{aligned}$$

Therefore, I_γ is not reduced. Also, I_γ is not ambiguous since $\frac{2P}{Q}=\frac{4-6p}{p-1}$ is not an integer for primes $p \geq 5$. □

Theorem 2.3. *The form* F_γ *in* (2.2) *is not reduced and is not ambiguous for any prime* $p \geq 5$.

Proof. We proved in the previous theorem that I_γ is not reduced, that is, $p-1>(2+3p)+\sqrt{p}$. Since $9p^2-13p+4>0$, we have

$$\begin{aligned} 9p^2-13p+4>0 &\Leftrightarrow 9p^2-12p+4>p \Leftrightarrow 2-3p>\sqrt{p} \\ &\Leftrightarrow 4-6p>\sqrt{4p} \Leftrightarrow b>\sqrt{\Delta}. \end{aligned}$$

So F_γ is not reduced by (1.2). For $g=[r;s;t;u] \in \overline{\Gamma}$, the system of equations

$$\begin{aligned} (p-1)r^2+(4-6p)rs+(9p-4)s^2 &= p-1, \\ (2p-2)rt+(4-6p)ru+(4-6p)ts+(18p-8)su &= 4-6p, \\ (p-1)t^2+(4-6p)tu+(9p-4)u^2 &= 9p-4 \end{aligned}$$

has no solution with $\det g=-1$. So F_γ is not improperly equivalent to itself and hence is not ambiguous. □

If an indefinite form F is not reduced, then we can get it into a reduced form by applying the following algorithm: Let $F=F_0=(a_0,b_0,c_0)$ and let $s_i=\operatorname{sign}(c_i)\left\lfloor\frac{b_i}{2|c_i|}\right\rfloor$ for $|c_i| \geq \sqrt{\Delta}$ or $\operatorname{sign}(c_i)\left\lfloor\frac{b_i+\sqrt{\Delta}}{2|c_i|}\right\rfloor$ for $|c_i|<\sqrt{\Delta}$ for $i \geq 0$. Then the reduction of F is

$$\rho^{i+1}(F)=(c_i,-b_i+2c_is_i,c_is_i^2-b_is_i+a_i) \tag{2.3}$$

for $i \geq 0$ (see [1]).

Now we consider the reduction of F_γ. Let $F_\gamma=F_{\gamma_0}=(p-1,4-6p,9p-4)$. Then $s_0=-1$ and hence $\rho^1(F_\gamma)=(9p-4,-12p+4,4p-1)$. Similarly, we obtain the following table where $t=\lfloor\sqrt{p}\rfloor$. So, we can give the following theorem.

Theorem 2.4. *The reduction of* F_γ *is* $\rho^4(F_\gamma)=(-1,2t,p-t^2)$, *where* $t=\lfloor\sqrt{p}\rfloor$.

Table 1.
Reduction of F_γ

i	a_i	b_i	c_i	s_i
0	$p-1$	$4-6p$	$9p-4$	-1
1	$9p-4$	$-12p+4$	$4p-1$	-1
2	$4p-1$	$4p-2$	$p-1$	2
3	$p-1$	-2	-1	$1-t$
4	-1	$2t$	$p-t^2$	

3. BINARY QUADRATIC FORMS OVER FINITE FIELDS

In the first section, we give some notation for binary quadratic forms. Now we generalize this notation to any finite field $\mathbb{F}_p$ for a primes $p \geq 5$. A binary quadratic form F^p over $\mathbb{F}_p$ is a form in two variables x and y of the type $F^p(x, y) = ax^2 + bxy + cy^2$, where $a, b, c \in \mathbb{F}_p$. We denote F^p briefly by $F^p = (a, b, c)$. The discriminant of F^p is defined by the formula $b^2 - 4ac$ and is denoted by $\Delta^p = \Delta^p(F^p)$. Set $\overline{\Gamma}^p = \{g^p = [r; s; t; u] : r, s, t, u \in \mathbb{F}_p$ and $ru - st \equiv \pm 1 (\operatorname{mod} p)\}$. Let F^p and G^p be two forms over $\mathbb{F}_p$. If there exists a $g^p \in \overline{\Gamma}^p$ such that $g^p F^p = G^p$, then F^p and G^p are called equivalent. If $\det g^p \equiv 1 (\operatorname{mod} p)$, then F^p and G^p are called properly equivalent and if $\det g^p \equiv -1 (\operatorname{mod} p)$, then F^p and G^p are called improperly equivalent. A form F^p is called ambiguous if it is improperly equivalent to itself. An element $g^p \in \overline{\Gamma}^p$ is called an automorphism of F^p if $g^p F^p = F^p$. If $\det g^p \equiv 1 (\operatorname{mod} p)$, then g is called a proper automorphism and if $\det g^p \equiv -1 (\operatorname{mod}\ p)$, then g is called an improper automorphism. Let $\operatorname{Aut}(F^p)^{p,+}$ denote the set of proper automorphisms of F^p and let $\operatorname{Aut}(F^p)^{p,-}$ denote the set of improper automorphisms of F^p.

Recall that $F_\gamma = (p-1, 4-6p, 9p-4)$. If we consider this form over $\mathbb{F}_p$, then we obtain

$$F_\gamma^p = (p-1, 4, p-4). \tag{3.1}$$

First we consider the proper and improper automorphisms of F_γ^p.

Theorem 3.1. *Let F_γ^p be the form defined in* (3.1). *Then*

$$\# \operatorname{Aut}(F_\gamma^p)^{p,+} = \# \operatorname{Aut}(F_\gamma^p)^{p,-} = 2p$$

for every primes $p \geq 5$.

Proof. First we consider the proper automorphisms. Let $p = 5$. Then $F_\gamma^5 = (4, 4,\ 1)$. Let $g^p = [r; s; t; u] \in \overline{\Gamma}^5$. Then by (1.3), we have the following system of equations

$$
\begin{aligned}
4r^2+4rs+s^2&=4\\
8rt+4ru+4ts+2su&=4 \qquad (3.2)\\
4t^2+4tu+u^2&=1.
\end{aligned}
$$

This system has a solution for $g^5=[0;2;2;2],[0;3;3;3],[1;0;0;1],[1;1;1;2],[2;3;3;0],[2;4;4;1],[3;1;1;4],[3;2;2;0],[4;0;0;4]$ and $[4;4;4;3]$. Note that $\det g^5=1$. So,

$$\operatorname{Aut}(F^5_\gamma)^{5,+}=\left\{\begin{array}{c}[0;2;2;2],[0;3;3;3],[1;0;0;1],[1;1;1;2],[2;3;3;0],\\ [2;4;4;1],[3;1;1;4],[3;2;2;0],[4;0;0;4],[4;4;4;3]\end{array}\right\}$$

and hence $\#\operatorname{Aut}(F^5_\gamma)^{5,+}=10$. Also (3.2) has a solution for $g^5=[0;2;3;0],[0;3;2;0],[1;0;1;4],[1;1;0;4],[2;3;4;3],[2;4;3;3],[3;1;2;2],[3;2;1;2],[4;0;4;1]$ and $[4;4;0;1]$ with $\det g^5=-1$. So,

$$\operatorname{Aut}(F^5_\gamma)^{5,-}=\left\{\begin{array}{c}[0;2;3;0],[0;3;2;0],[1;0;1;4],[1;1;0;4],[2;3;4;3],\\ [2;4;3;3],[3;1;2;2],[3;2;1;2],[4;0;4;1],[4;4;0;1]\end{array}\right\}$$

and hence $\#\operatorname{Aut}(F^5_\gamma)^{5,-}=10$.

Similarly, it can be shown that $\#\operatorname{Aut}(F^p_\gamma)^{p,+}=\#\operatorname{Aut}(F^p_\gamma)^{p,-}=2p$ for every primes $p\geq 7$. □

3.1. Representation of integers by quadratic forms

Representations of integers (or primes) by binary quadratic forms have an important role on the theory of numbers and are studied by many authors. In fact, this problem intimately connected with reciprocity laws. The major problem of the theory of quadratic forms is: given a quadratic form F, find all integers n that can be represented by F, that is, for which the equation $F(x,y)=ax^2+bxy+cy^2=n$ has a solution (x,y). This problem was studied for specific quadratic forms by Fermat, and intensively investigated by Euler. Fermat considered the representation of integers as sums of two squares. It was, however, Gauss in the Disquisitions [6] who made the fundamental breakthrough and developed a comprehensive and beautiful theory of binary quadratic forms. Most important was his definition of the composition of two forms and his proof that the (equivalence classes of) forms with a given discriminant Δ form a commutative group under this composition. The idea behind composition of forms is simple. If forms F and G represent integers n and m, respectively, then their composition $F*G$ should represent $n\cdot m$. The implementation of this idea is subtle and extremely difficult to describe. Attempts to gain conceptual insight into Gauss theory of composition of forms inspired the efforts of some of the best mathematicians of the time, among them Dirichlet, Kummer and Dedekind. The main ideal here was to extend the domain of higher arithmetic and view the problem in a broader context.

In this subsection, we will consider the the number of representations of integers $n \in \mathbb{F}_p^*$ by F_γ^p defined in (3.1). It is known that [7], to each quadratic form F, there corresponds the theta series

$$\wp(\tau; F) = 1 + \sum_{n=1}^{\infty} r(n; F) z^n, \tag{3.3}$$

where $r(n; F)$ is the number of representations of a positive integer n by the quadratic form F and $z = \exp(2\pi i\tau)$ for $\mathrm{Im}(\tau) > 0$. We can generalize (3.3) to any finite field $\mathbb{F}_p$. Let $F^p = (a, b, c)$ be a quadratic form over $\mathbb{F}_p$ for $a, b, c \in \mathbb{F}_p$. Then (3.3) becomes

$$\wp^p(\tau; F^p) = 1 + \sum_{n \in \mathbb{F}_p^*} r^p(n; F^p) z^n, \tag{3.4}$$

where $r^p(n; F^p)$ is the number of representations of $n \in \mathbb{F}_p^*$ by F^p. Note that the theta series in (3.4) is determined by $r^p(n; F^p)$. So, we have the find out $r^p(n; F^p)$. Let Q_p denote the set of quadratic residues mod p. Then we have the following theorem.

Theorem 3.2. *Let F_γ^p be the quadratic form. If $p \equiv 1 (\bmod 4)$, then*

$$r^p(n; F_\gamma^p) = \begin{cases} \#\,\mathrm{Aut}(F_\gamma^p)^{p,+} & \text{if } n \in Q_p, \\ 0 & \text{if } n \notin Q_p \end{cases}$$

and if $p \equiv 3 (\bmod 4)$, then

$$r^p(n; F_\gamma^p) = \begin{cases} 0 & \text{if } n \in Q_p, \\ \#\,\mathrm{Aut}(F_\gamma^p)^{p,+} & \text{if } n \notin Q_p. \end{cases}$$

Proof. Let $p \equiv 1 (\bmod 4)$. Then $(\frac{-1}{p}) = 1$, where $(\frac{\cdot}{p})$ denotes the Legendre symbol. Let $x \in \mathbb{F}_p$ be given. Then we want to solve the quadratic congruence

$$(p-1)x^2 + 4xy + (p-4)y^2 \equiv n (\bmod p) \tag{3.5}$$

according to y. From (3.5), we get

$$(p-4)y^2 + 4xy + (p-1)x^2 - n \equiv 0 (\bmod p). \tag{3.6}$$

The discriminant of (3.6) is $\Delta = (4xy)^2 - 4(p-4)((p-1)x^2 - n) \equiv -16n (\bmod p)$. So, the solutions of (3.6) are

$$y_{1,2} = \frac{-4x \pm \sqrt{\Delta}}{2(p-4)} \equiv \frac{-4x \pm \sqrt{-16n}}{2(p-4)} \equiv \frac{-2x \pm 2\sqrt{-n}}{p-4}. \tag{3.7}$$

Note that -1 is a quadratic residue when $p \equiv 1 (\mathrm{mod}\, 4)$. So, (3.7) becomes

$$y_{1,2} \equiv \frac{-2x \pm 2\sqrt{n}}{p-4}. \tag{3.8}$$

If $n \in Q_p$, then $\sqrt{n} \in \mathbb{F}_p^*$. So there are two solutions $y_{1,2}$. Therefore, there are $2p$ integer solutions of (3.6). If $n \notin Q_p$, then $\sqrt{n} \notin \mathbb{F}_p^*$. So, there are no integer solutions $y_{1,2}$. The second case can be proved similarly. □

We proved in Theorem 2.4 the reduction of F_γ is $\rho^4(F_\gamma) = (-1, 2t, p-t^2)$ for $t = \lfloor \sqrt{p} \rfloor$. If we consider $\rho^4(F_\gamma)$ over $\mathbb{F}_p$, then we get

$$\rho^{p,4}(F_\gamma^p) = (p-1, 2t, p-t^2). \tag{3.9}$$

Now, we can give the following theorems without giving its proof since they can be proved as in the same way that Theorems 3.1 and 3.2 were proved.

Theorem 3.3. *Let $\rho^{p,4}(F_\gamma^p)$ be the quadratic form in* (3.9). *Then*

$$\#\,\mathrm{Aut}(\rho^{p,4}(F_\gamma^p))^{p,+} = \#\,\mathrm{Aut}(\rho^{p,4}(F_\gamma^p))^{p,-} = 2p$$

for any prime $p \geq 5$.

Theorem 3.4. *Let $\rho^{p,4}(F_\gamma^p)$ be the quadratic form. If $p \equiv 1(\mathrm{mod}\, 4)$, then*

$$r^p(n; \rho^{p,4}(F_\gamma^p)) = \begin{cases} \#\,\mathrm{Aut}(\rho^{p,4}(F_\gamma^p))^{p,+} & \text{if } n \in Q_p, \\ 0 & \text{if } n \notin Q_p \end{cases}$$

and if $p \equiv 3(\mathrm{mod}\, 4)$, then

$$r^p(n; \rho^{p,4}(F_\gamma^p)) = \begin{cases} 0 & \text{if } n \in Q_p, \\ \#\,\mathrm{Aut}(\rho^{p,4}(F_\gamma^p))^{p,+} & \text{if } n \notin Q_p. \end{cases}$$

***n*-Universal Form.** In this subsection, we will consider the representation of integers by quadratic forms. First we define the following: let F^p be a quadratic form over $\mathbb{F}_p$ and let $n \in \mathbb{F}_p^*$. If n can be represented by F^p, then F^p is called n-universal form. Now we can give the following theorem.

Theorem 3.5. *Let F_γ^p be the form in* (3.1). *Then F_γ^p*
(1) *is a* 1*-universal form if $p \equiv 1(\mathrm{mod}\, 4)$;*
(2) *is a* 2*-universal form if $p \equiv 1, 3(\mathrm{mod}\, 8)$;*
(3) *is a* 3*-universal form if $p \equiv 1, 7(\mathrm{mod}\, 12)$;*
(4) *is a* 4*-universal form if $p \equiv 1, 5(\mathrm{mod}\, 12)$;*
(5) *is a* 5*-universal form if $p \equiv 1, 3, 7, 9(\mathrm{mod}\, 20)$;*
(6) *is a* 6*-universal form if $p \equiv 1, 5, 7, 11, 25, 29, 31, 35(\mathrm{mod}\, 48)$;*
(7) *is a* 7*-universal form if $p \equiv 1, 9, 11, 15, 23, 25(\mathrm{mod}\, 28)$;*
(8) *is a* 8*-universal form if $p \equiv 1, 11, 17, 19, 25, 35, 41, 43(\mathrm{mod}\, 48)$;*
(9) *is a* 9*-universal form if $p \equiv 1, 5, 13, 17(\mathrm{mod}\, 24)$;*
(10) *is a* 10*-universal form if $p \equiv 1, 7, 9, 11, 13, 19, 23, 37(\mathrm{mod}\, 40)$;*

(11) *is a* $\frac{p-1}{2}$*-universal form if* $p \equiv 1, 3 (\bmod 8)$;
(12) *is a* $(p-1)$*-universal form for every primes* $p \geq 5$;
(13) *is a* $(p-2)$*-universal form if* $p \equiv 1, 7 (\bmod 8)$;
(14) *is a* $(p-3)$*-universal form if* $p \equiv 1, 11 (\text{mod } 12)$;
(15) *is a* $(p-4)$*-universal form for every primes* $p \geq 5$;
(16) *is a* $(p-5)$*-universal form if* $p \equiv 1, 9 (\bmod 10)$;
(17) *is a* $(p-6)$*-universal form if* $p \equiv 1, 5, 19, 23 (\bmod 24)$;
(18) *is a* $(p-7)$*-universal form if* $p \equiv 1, 3, 9, 19, 25, 27 (\bmod 28)$;
(19) *is a* $(p-8)$*-universal form if* $p \equiv 1, 7, 17, 23 (\bmod 24)$;
(20) *is a* $(p-9)$*-universal form for every primes* $p \geq 11$;
(21) *is a* $(p-10)$*-universal form if* $p \equiv 1, 3, 9, 13, 27, 31, 37, 39 (\text{mod } 40)$;
(22) *is not a* p*-universal form for every primes* $p \geq 5$.

Proof. 1. Recall that $n^{(p-1)/2} = 1$ if $n \in Q_p$ and $n^{(p-1)/2} = -1$ if $n \notin Q_p$ for $n \in \mathbb{F}_p^*$, that is, $\left(\frac{n}{p}\right) = n^{(p-1)/2}$. Further, let $\left\{n, 2n, 3n, \ldots, \frac{p-1}{2}n\right\}$ be the set of multiplies of n. Represent each of these elements of $\mathbb{F}_p$ by an integer in the range $\left(\frac{-p}{2}, \frac{p}{2}\right)$ and let v denote the number of negative integers in this set. Then $\left(\frac{n}{p}\right) = (-1)^v$. Now let $p \geq 5$ be any prime number. Then $p-1$ is always even. Hence $\left(\frac{1}{p}\right) = 1$ for every primes p. Now consider the set $\{2, 4, 6, \ldots, p-1\}$. We know that 2 is an quadratic residue $\bmod\, p$ if and only if v lie in the interval $\left(-\frac{p}{2}, 0\right)$ is even. Note that v is the number of even integers in the interval $\left[\frac{p+1}{2}, p-1\right]$. Let $\frac{p+1}{2}$ is even. Then $p \equiv 3 (\bmod 4)$ and hence $v = \frac{(p-1)-\frac{p+1}{2}}{2} + 1 = \frac{p+1}{4}$. So $\left(\frac{2}{p}\right) = 1$ if $p \equiv 7 (\bmod 8)$ or -1 if $p \equiv 3 (\bmod 8)$. Similarly let $\frac{p+1}{2}$ is odd. Then $p \equiv 1 (\bmod 4)$ and hence $v = \frac{(p-1)-\frac{p+3}{2}}{2} + 1 = \frac{p-1}{4}$. Therefore $\left(\frac{2}{p}\right) = 1$ if $p \equiv 1 (\bmod 8)$ of -1 if $p \equiv 5 (\bmod 8)$. Consequently, we get $\left(\frac{2}{p}\right) = 1$ if $p \equiv 1, 7 (\bmod 8)$ or -1 if $p \equiv 3,\ 5 (\bmod 8)$. Similarly it can be shown that $\left(\frac{3}{p}t\right) = 1$ if $p \equiv 1, 11 (\bmod 12)$ or -1 if $p \equiv 5, 7 (\bmod 12)$; $\left(\frac{4}{p}\right) = 1$ for any prime $p \geq 5$; $\left(\frac{5}{p}\right) = 1$ if $p \equiv 1, 9 (\bmod 10)$ or -1 if $p \equiv 3, 7 (\bmod 10)$; $\left(\frac{6}{p}\right) = 1$ if $p \equiv 1, 5, 19, 23 (\bmod 24)$ or -1 if $p \equiv 7, 11, 13, 17 (\bmod 24)$; $\left(\frac{7}{p}\right) = 1$ if $p \equiv 1, 3, 9, 19, 25, 27 (\bmod 28)$ or -1 if $p \equiv 5, 11, 13, 15, 17, 23 (\bmod 28)$; $\left(\frac{8}{p}\right) = 1$ if $p \equiv 1, 7, 17, 23 (\bmod 24)$ of -1 if $p \equiv 5, 11, 13, 19 (\bmod 24)$; $\left(\frac{9}{p}\right) = 1$ for every primes $p \geq 11$; $\left(\frac{10}{p}\right) = 1$ if $p \equiv 1, 3, 9, 13, 27, 31, 37, 39 (\bmod 40)$ or -1

if $p \equiv 7,\ 11, 17, 19, 21, 23, 29, 33, 37 (\operatorname{mod} 40)$ and $\left(\frac{\frac{p+1}{2}}{p}\right) = 1$ if $p \equiv 1, 3 (\operatorname{mod} 8)$ or -1 if $p \equiv 5,\ 7 (\operatorname{mod} 8)$.

With the same argument, we find that $-1 \in Q_p \Leftrightarrow p \equiv 1 (\operatorname{mod} 4)$; $-2 \in Q_p \Leftrightarrow p \equiv 1, 3 (\operatorname{mod} 8)$; $-3 \in Q_p \Leftrightarrow p \equiv 1, 7 (\operatorname{mod} 12)$; $-4 \in Q_p \Leftrightarrow p \equiv 1, 5 (\operatorname{mod} 12)$; $-5 \in Q_p \Leftrightarrow p \equiv 1, 3, 7, 9 (\operatorname{mod} 20)$; $-6 \in Q_p \Leftrightarrow p \equiv 1, 5, 7, 11, 25, 29, 31, 35 (\operatorname{mod} 48)$; $-7 \in Q_p \Leftrightarrow p \equiv 1, 9, 11, 15, 23, 25 (\operatorname{mod} 28)$; $-8 \in Q_p \Leftrightarrow p \equiv 1, 11, 17, 19, 25, 35, 41, 43 (\bmod\ 48)$; $-9 \in Q_p \Leftrightarrow p \equiv 1, 5, 13, 17$ $(\bmod\ 24)$; $-10 \in Q_p \Leftrightarrow p \equiv 1, 7, 9, 11, 13, 19, 23, 37 (\operatorname{mod} 40)$. Applying the Theorem 3.2 the results from 1 to 21 are obvious.

22. Now let $p \geq 5$ be a prime. Then the quadratic equation

$$F_\gamma^p(x, y) = (p - 1)x^2 + 4xy + (p - 4)y^2 \equiv p (\operatorname{mod} p)$$

has no solution (x, y). Therefore, F_γ^p is not a p-universal form any prime $p \geq 5$. $\square$

4. RATIONAL POINTS ON ELLIPTIC CURVES OVER FINITE FIELDS

In this section, we will consider the rational points on elliptic curves associated to F_γ^p obtained in the previous section. Recall that an elliptic curve E over a finite field $\mathbb{F}_p$ is defined by an equation in the Weierstrass form

$$E : y^2 = x^3 + ax^2 + bx, \tag{4.1}$$

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

$$\#E(\mathbb{F}_p) = p + 1 + \sum_{x \in \mathbb{F}_p} \left(\frac{x^3 + ax^2 + bx}{\mathbb{F}_p}\right), \tag{4.2}$$

where $\left(\frac{\cdot}{\mathbb{F}_p}\right)$ denotes the Legendre symbol (for the arithmetic of elliptic curves and rational points on them see [11, 13]).

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. To get this 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

$$E_F:\quad y^2=ax^3+bx^2+cx. \tag{4.3}$$

If we making the substitution $y'=ay$ and $x'=ax+2$ in (4.3), then we obtain

$$E_F:\quad y'^2=x'^3+(b-6)x'^2+(12-4b+ac)x'+(-8+4b-2ac). \tag{4.4}$$

Note that $F_\gamma^p=(p-1,4,p-4)$ and hence $-8+4b-2ac=-2p^2+10p\equiv 0(\operatorname{mod} p)$, that is, $ac=2b-4$. So (4.4) becomes

$$E_{F_\gamma^p}:\quad y'^2=x'^3+(b-6)x'^2+(8-2b)x'. \tag{4.5}$$

The discriminant of $E_{F_\gamma^p}$ is hence $\Delta(E_{F_\gamma^p})=64(b-2)^2\Delta(F)$ since $\Delta(F_\gamma^p)=(b-4)^2$. So, we have a correspondence between F_γ^p and $E_{F_\gamma^p}$. Since $F_\gamma^p=(p-1,4,p-4)$, this curve becomes

$$E_{F_\gamma^p}:\quad y'^2=x'^3-2x'^2=x'^2(x'-2) \tag{4.6}$$

which is a singular curve. Now we can give following lemma.

Lemma 4.1 ([8]). *Let p be an odd prime and let $f(x)\in\mathbb{Z}[x]$ be a polynomial of degree ≥ 1. Then the number $N_p(f)$ of solutions $(x,y)\in\mathbb{F}_p\times\mathbb{F}_p$ of the congruence $y^2\equiv f(x)(\operatorname{mod} p)$ is $N_p(f)=p+1+S_p(f)$, where*

$$S_p(f)=\sum_{x=0}^{p-1}\left(\frac{f(x)}{p}\right). \tag{4.7}$$

Also it is showed in [13] that for the polynomial $f(x)=(x-r)^2(x-s)$ of degree 3 for some $r,s\in\mathbb{F}_p$,

$$\sum_{x=0}^{p-1}\left(\frac{f(x)}{\mathbb{F}_p}\right)=-\left(\frac{r-s}{p}\right). \tag{4.8}$$

Applying (4.7) and (4.8), we deduce that

$$\#E_{F_\gamma^p}(\mathbb{F}_p)=p+1+\sum_{x=0}^{p-1}\left(\frac{x'^2(x'-2)}{\mathbb{F}_p}\right)=p+1-\left(\frac{-2}{p}\right). \tag{4.9}$$

Hence we can give following theorem.

Theorem 4.2. *For the curve $E_{F_\gamma^p}$ in (4.6), we have*

$$\#E_{F_\gamma^p}(\mathbb{F}_p)=\begin{cases} p & \text{if } p\equiv 1,3(\operatorname{mod} 8),\\ p+2 & \text{if } p\equiv 5,7(\operatorname{mod} 8)\end{cases}$$

for any prime $p\geq 5$.

Proof. Note that in (4.9), the order of $E_{F_\gamma^p}$ is p or $p+2$ if -2 is a quadratic residue mod p or not, respectively. Therefore, the determination of the order of $E_{F_\gamma^p}$ depends on when -2 is a quadratic residue or not. We see in the previous section that $(\frac{-2}{p}) = 1$ if $p \equiv 1, 3 (\bmod 8)$ and $(\frac{-2}{p}) = -1$ if $p \equiv 5, 7 (\bmod 8)$. So the result is clear by (4.9). □

REFERENCES

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

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

[3] J.H. Conway, *Universal Quadratic Forms and the Fifteen Theorem, Quadratic Forms and their Applications.* (Dublin), Contemp. Math. **272**, Amer. Math. Soc., Providence, RI (2000), 23–26.

[4] L.E. Dickson, *Universal Quadratic Forms.* Transactions of the American Mathematical Society **31**(1) (1929), 164–189.

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

[6] C.F. Gauss, *Disquisitiones Arithmeticae.* English translation by Arthur A. Clarke, Yale University Press, 1966.

[7] E. Hecke, *Mathematische Werke.* Zweite Auflage, Vandenhoeck u. Ruprecht. Göttingen, 1970.

[8] F. Lemmermeyer, *Reciprocity Laws. From Euler to Eisenstein.* Springer-Verlag, Heidelberg, 2000.

[9] R.A. Mollin, *Quadratics.* CRS Press, Boca Raton, New York–London–Tokyo, 1996.

[10] O.T. O'Meara, *Introduction to Quadratic Forms.* Springer Verlag, New York, 1973.

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

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

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

Received 23 November 2009

Uludag University
Faculty of Science
Department of Mathematics
Görükle 16059, Bursa-Turkiye
tekcan@uludag.edu.tr
aozkoc@uludag.edu.tr