n-Universal Quadratic Forms and Quadratic Forms over Finite Fields

AHMET TEKCAN AND ARZU ÖZKOÇ

Abstract. In this work, we derive some properties of n-universal quadratic forms and quadratic forms over finite fields $\mathbb{F}_p$ for primes $p \geq 5$.

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

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

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

$$gF(x, y) = \left(ar^2 + brs + cs^2\right) x^2 + (2art + bru + bts + 2csu)\, xy + \left(at^2 + btu + cu^2\right) y^2 \tag{1.2}$$

for $g = \begin{pmatrix} r & s \\ t & u \end{pmatrix} = [r; s; t; u] \in \overline{\Gamma}$, that is, gF is obtained from F by making the substitution $x \to rx + tu, y \to sx + uy$. Moreover,

2000 *Mathematics Subject Classification.* 11E04,11E16, 11E18.

Key words and phrases. Quadratic form, quadratic irrational, quadratic ideal, universal form.

$\Delta(F) = \Delta(gF)$ 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 $Aut(F)^+$ denote the set of proper automorphisms of F and let $Aut(F)^-$ denote the set of improper automorphisms of F.

2. Quadratic Irrationals, Quadratic Ideals and Quadratic Forms

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 (see [3, 4]).

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 $(x, y) = (2-3n, n-1)$. Let $p \geq 5$ be a prime number. Then p can be represented by F. Now 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

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

is a quadratic ideal. I_γ is called reduced if $P + \sqrt{D} > Q$ and $-Q < P - \sqrt{D} < 0$ and is called ambiguous if and only if $\frac{2P}{Q} \in \mathbb{Z}$. Mollin considered the arithmetic of quadratic irrationals and quadratic ideals in his book [8]. He proved that given an ideal $I_\gamma = [Q, P + \sqrt{D}]$, there exists an indefinite binary quadratic form

$$F_\gamma(x, y) = Qx^2 + 2Pxy + \left(\frac{P^2 - D}{Q}\right) y^2 \tag{2.2}$$

of discriminant $\Delta = 4D$. Hence there is a correspondence between ideals and quadratic forms.

Theorem 2.1. *The ideal I_γ in* (2.1) *is not reduced and is not ambiguous for every 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

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

Hence 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 the ideal I_γ, the corresponding quadratic form is hence

$$F_\gamma(x,y)=(p-1)x^2+(4-6p)xy+(9p-4)y^2 \tag{2.3}$$

by (2.2).

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

Proof. We proved in Theorem 2.1 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. Also 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 for $g=[r;s;t;u] \in \overline{\Gamma}$ with $\det g=-1$. So F_γ is not improperly equivalent to itself and hence is not ambiguous. □

Recall that if a form F is not reduced, then we can get it into a reduced form as follows: Let $F=(a,b,c)$ be an indefinite form and let $\Omega=\{[1;s;0;1] : s \in \mathbb{Z}\}$. Then Ω is a cyclic subgroup of $\mathrm{SL}(2,\mathbb{Z})$

which is generated by $S = [1; 1; 0; 1]$. Now we want to determine the element in the Ω-orbit of F for which the absolute value of xy is minimal. For $s \in \mathbb{Z}$, we have

$$S^s F = (a, b + 2sa, as^2 + bs + c). \tag{2.4}$$

Hence the coefficient of x^2 of any form in the Ω-orbit of F is a and the coefficient of xy of such a form is uniquely determined $(\mathrm{mod}\, 2a)$. 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 (2.4), the coefficient of y^2 in $S^s F$ is $\frac{(2as+b)^2+|\Delta|}{4a}$. So this choices of s minimizes this coefficient. Hence the form $F = (a, b, c)$ is called normal if $-|a| < b \leq |a|$ for $|a| \geq \sqrt{\Delta}$ or $\sqrt{\Delta} - 2|a| < b < \sqrt{\Delta}$ for $|a| < \sqrt{\Delta}$. We see as above that, the $\Omega-$orbit of F contains one normal form which can be obtained as $S^s F$ with $s = \left\lfloor \frac{a-b}{2a} \right\rfloor$. The normal form in the Ω-orbit of F is called the normalization of F, which means replacing F by its normalization. Let $\rho(F)$ denotes the normalization of $(c, -b, a)$, let $F = F_0 = (a_0, b_0, c_0)$ and let

$$s_i = \begin{cases} sign(c_i) \left\lfloor \frac{b_i}{2|c_i|} \right\rfloor & \text{for } |c_i| \geq \sqrt{\Delta} \\ \\ sign(c_i) \left\lfloor \frac{b_i + \sqrt{\Delta}}{2|c_i|} \right\rfloor & \text{for } |c_i| < \sqrt{\Delta} \end{cases} \tag{2.5}$$

for $i \geq 0$. Then by (2.4), the reduction of F is

$$\rho^{i+1}(F) = (c_i, -b_i + 2c_i s_i, c_i s_i^2 - b_i s_i + a_i) \tag{2.6}$$

for $i \geq 0$. In this case, the form $\rho^j(F)$ is called the reduction of F (see [1]).

Now we can consider the reduction of F_γ.

Theorem 2.3. *The reduction of F_γ is $\rho^4(F_\gamma) = (-1, 2t, p - t^2)$, where $t = \lfloor \sqrt{p} \rfloor$.*

Proof. Let $F_\gamma = F_{\gamma_0} = (p - 1, 4 - 6p, 9p - 4)$. Then by (2.5), we get $s_0 = -1$ and hence by (2.6), we get $\rho^1(F_\gamma) = (9p-4, -12p+4, 4p-1)$. But $\rho^1(F_\gamma)$ is not reduced. So we can apply the reduction algorithm again, then we find that $s_1 = -1$ and hence $\rho^2(F_\gamma) = (4p - 1, 4p - 2, p - 1)$. Similarly $\rho^2(F_\gamma)$ is not reduced. If we continue, then we find that $s_2 = 2$ and hence $\rho^3(F_\gamma) = (p-1, -2, -1)$. Again $\rho^3(F_\gamma)$ is not reduced. If we continue, then we find $s_3 = 1-t$, where $t = \lfloor \sqrt{p} \rfloor$, and hence $\rho^4(F_\gamma) = (-1, 2t, p - t^2)$. This form is reduced. □

3. Binary Quadratic Forms over Finite Fields

In the first section, we gave some notation on binary quadratic forms. Now we generalize these to any finite field $\mathbb{F}_p$ for a prime $p \geq 5$. A binary quadratic form F^p over $\mathbb{F}_p$ is a form in two variables x and y of the type

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

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

$$\overline{\Gamma}^p = \{g^p = [r; s; t; u] : r, s, t, u \in \mathbb{F}_p \text{ and } ru - st \equiv \pm 1 (\text{mod } p)\}.$$

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 $\det g^p = 1$, then F^p and G^p are called properly equivalent and if $\det g^p = p - 1$, 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 $\det g^p = 1$, then g is called a proper automorphism and if $\det g^p = -1$, then g is called an improper automorphism. Let $Aut(F^p)^{p,+}$ denote the set of proper automorphisms of F^p and let $Aut(F^p)^{p,-}$ 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 a form defined in* (3.1)*. Then*

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

for every prime $p \geq 5$.

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), we have the following system of equations:

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

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

$$Aut(F_\gamma^5)^{5,+} = \left\{ \begin{matrix} [0;2;2;2], [0;3;3;3], [1;0;0;1], [1;1;1;2], [2;3;3;0], \\ [2;4;4;1], [3;1;1;4], [3;2;2;0], [4;0;0;4], [4;4;4;3] \end{matrix} \right\}$$

and hence $\#Aut(F_\gamma^5)^{5,+} = 10$.

The system of equations in (3.2) has a solution for $g^p = [0;2;3;0], [0;3;2;0], [1;0;1;4], [1;1;0;4], [2;3;4;3], [2;4;3;3], [3;1;2;2], [3;2;1;2], [4;0;4;1]$ and $[4;4;0;1]$ with $\det g^p = -1$. So

$$Aut(F_\gamma^5)^{5,-} = \left\{ \begin{matrix} [0;2;3;0], [0;3;2;0], [1;0;1;4], [1;1;0;4], [2;3;4;3], \\ [2;4;3;3], [3;1;2;2], [3;2;1;2], [4;0;4;1], [4;4;0;1] \end{matrix} \right\}$$

and hence $\#Aut(F_\gamma^5)^{5,-} = 10$. Similarly it can be shown that $\#Aut(F_\gamma^p)^{p,+} = \#Aut(F_\gamma^p)^{p,-} = 2p$ for every prime $p \geq 7$. □

Now we consider the representation problem. 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 to reciprocity laws. The major problem of the theory of quadratic forms was: 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.

Now we will consider the the number of representations of integers $n \in \mathbb{F}_p^*$ by quadratic forms 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 $Im(\tau) > 0$. Now

we 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.*

(1) *If $p \equiv 1 (\text{mod } 4)$, then*

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

(2) *If $p \equiv 3 (\text{mod } 4)$, then*

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

Proof. (1) Let $p \equiv 1 (\text{mod } 4)$. 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

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

according to y. From (3.5), we get

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

The discriminant of (3.6) is $\Delta = (4xy)^2 - 4(p-4)((p-1)x^2 - n) \equiv -16n (\text{mod } p)$. 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 $p \equiv 1 (\text{mod } 4)$. 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 $y_{1,2}$.

(2) It can be proved as in the same way that (1) was proved. □

We proved in Theorem 2.3 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 it 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*

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

for every prime $p \geq 5$.

Theorem 3.4. *Let $\rho^{p,4}(F_\gamma^p)$ be the quadratic form*

(1) *If $p \equiv 1 (\mathrm{mod}\ 4)$, then*

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

(2) *If $p \equiv 3 (\mathrm{mod}\ 4)$, then*

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

4. $n-$Universal Form

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 4.1. *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 an 8-universal form if $p \equiv 1, 11, 17, 19, 25, 35, 41 (\mathrm{mod}\, 48)$, or if $p \equiv 43 (\mathrm{mod}\, 48)$*
(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* $p \equiv 1, 3 (\mathrm{mod}\, 8)$
(12) *is a* $(p-1)$*-universal form for every prime* $p \geq 5$
(13) *is a* $(p-2)$*-universal form if* $p \equiv 1, 7 (\mathrm{mod}\, 8)$
(14) *is a* $(p-3)$*-universal form if* $p \equiv 1, 11 (\mathrm{mod}\ 12)$
(15) *is a* $(p-4)$*-universal form for every prime* $p \geq 5$
(16) *is a* $(p-5)$*-universal form if* $p \equiv 1, 9 (\mathrm{mod}\, 10)$
(17) *is a* $(p-6)$*-universal form if* $p \equiv 1, 5, 19, 23 (\mathrm{mod}\, 24)$
(18) *is a* $(p-7)$*-universal form if* $p \equiv 1, 3, 9, 19, 25, 27 (\mathrm{mod}\ 28)$
(19) *is a* $(p-8)$*-universal form if* $p \equiv 1, 7, 17, 23 (\mathrm{mod}\, 24)$
(20) *is a* $(p-9)$*-universal form for every prime* $p \geq 11$
(21) *is a* $(p-10)$*-universal form if* $p \equiv 1, 3, 9, 13, 27, 31 (\mathrm{mod}\ 40)$, *or if* $p \equiv 37, 39 (\mathrm{mod}\ 40)$
(22) *is not a* p*-universal form for every prime* $p \geq 5$.

Proof. 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, $(\frac{n}{p}) = n^{(p-1)/2}$. 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 $(\frac{n}{p}) = (-1)^v$. Now let $p \geq 5$ be any prime number. Then $p-1$ is always even. Hence $(\frac{1}{p}) = 1$ for every prime p.

Now consider the set $\{2, 4, 6, \ldots, p-1\}$. We know that 2 is an quadratic residue $\mathrm{mod}\, p$ if and only if v lie in the interval $(-\frac{p}{2}, 0)$ 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 $p \equiv 3 (\mathrm{mod}\, 4)$ and hence $v = \frac{(p-1)-\frac{p+1}{2}}{2} + 1 = \frac{p+1}{4}$. So

$$\left(\frac{2}{p}\right) = (-1)^{(p+1)/4} = \begin{cases} 1 & \text{if } p \equiv 7 (\mathrm{mod}\, 8) \\ -1 & \text{if } p \equiv 3 (\mathrm{mod}\, 8). \end{cases} \tag{4.1}$$

Similarly let $\frac{p+1}{2}$ is odd. Then $p \equiv 1 (\mathrm{mod}\, 4)$ and hence

$$v = \frac{(p-1) - \frac{p+3}{2}}{2} + 1 = \frac{p-1}{4}.$$

Therefore

$$\left(\frac{2}{p}\right) = (-1)^{(p-1)/4} = \begin{cases} 1 & \text{if } p \equiv 1 (\mathrm{mod}\, 8) \\ -1 & \text{if } p \equiv 5 (\mathrm{mod}\, 8). \end{cases} \tag{4.2}$$

Combining (4.1) and (4.2), we get $(\frac{2}{p}) = 1$ if $p \equiv 1, 7 (\mathrm{mod}\, 8)$ or -1 if $p \equiv 3, 5 (\mathrm{mod}\, 8)$.

Similarly it can be shown that $(\frac{3}{p}) = 1$ if $p \equiv 1, 11 (\mathrm{mod}\, 12)$ or -1 if $p \equiv 5, 7 (\mathrm{mod}\, 12)$; $(\frac{4}{p}) = 1$ for every prime $p \geq 5$; $(\frac{5}{p}) = 1$ if $p \equiv 1, 9 (\mathrm{mod}\, 10)$ or -1 if $p \equiv 3, 7 (\mathrm{mod}\, 10)$; $(\frac{6}{p}) = 1$ if $p \equiv 1, 5, 19, 23 (\mathrm{mod}\, 24)$ or -1 if $p \equiv 7, 11, 13, 17 (\mathrm{mod}\, 24)$; $(\frac{7}{p}) = 1$ if $p \equiv 1, 3, 9,\ 19, 25, 27 (\mathrm{mod}\, 28)$ or -1 if $p \equiv 5, 11, 13, 15, 17, 23 (\mathrm{mod}\, 28)$; $(\frac{8}{p}) = 1$ if $p \equiv 1, 7, 17, 23 (\mathrm{mod}\, 24)$ or -1 if $p \equiv 5, 11, 13, 19 (\mathrm{mod}\, 24)$; $(\frac{9}{p}) = 1$ for every prime $p \geq 11$; $(\frac{10}{p}) = 1$ if $p \equiv 1, 3, 9,\ 13, 27, 31, 37, 39 (\mathrm{mod}\, 40)$ or -1 if $p \equiv 7, 11, 17, 19, 21, 23, 29, 33, 37 (\mathrm{mod}\, 40)$ and $(\frac{\frac{p+1}{2}}{p}) = 1$ if $p \equiv 1, 3 (\mathrm{mod}\, 8)$ or -1 if $p \equiv 5, 7 (\mathrm{mod}\, 8)$.

With the same argument, we find that $(\frac{-1}{p}) = 1$ if $p \equiv 1 (\mathrm{mod}\ 4)$; $(\frac{-2}{p}) = 1$ if $p \equiv 1, 3 (\mathrm{mod}\ 8)$; $(\frac{-3}{p}) = 1$ if $p \equiv 1, 7 (\mathrm{mod}\ 12)$; $(\frac{-4}{p}) = 1$ if $p \equiv 1, 5 (\mathrm{mod}\ 12)$; $(\frac{-5}{p}) = 1$ if $p \equiv 1, 3, 7, 9 (\mathrm{mod}\ 20)$; $(\frac{-6}{p}) = 1$ if $p \equiv 1, 5, 7, 11, 25, 29, 31, 35 (\mathrm{mod}\ 48)$; $(\frac{-7}{p}) = 1$ if $p \equiv 1, 9, 11, 15, 23, 25 (\mathrm{mod}\ 28)$; $(\frac{-8}{p}) = 1$ if $p \equiv 1, 11,\ 17, 19,\ 25, 35,\ 41, 43 (\mathrm{mod}\ 48)$; $(\frac{-9}{p}) = 1$ if $p \equiv 1, 5, 13, 17 (\mathrm{mod}\ 24)$ and $(\frac{-10}{p}) = 1$ if $p \equiv 1, 7, 9,\ 11, 13,\ 19, 23,\ 37 (\mathrm{mod}\ 40)$.

We proved in Theorem 3.2 that if $p \equiv 1 (\mathrm{mod}\ 4)$, then

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

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

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

Combining this, the results from (1) to (21) are obvious.

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

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

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

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, Clasical 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] R.A. Mollin. *Quadratics.* CRS Press, Boca Raton, New York, London, Tokyo, 1996.
[9] O.T. O'Meara. *Introduction to Quadratic Forms.* Springer Verlag, New York, 1973.
[10] A. Tekcan and O. Bizim *The Connection Between Quadratic Forms and the Extended Modular Group.* Mathematica Bohemica **128**(3) (2003), 225–236.

Ahmet Tekcan and Arzu Özkoç,
Department of Mathematics,
Faculty of Science,
Uludag University,
Görükle 16059, Bursa, Turkey
tekcan@uludag.edu.tr; aozkoc@uludag.edu.tr

Received on 10 November 2008.