Irish Math. Soc. Bulletin **58** *(2006), 69–79*

On the Quadratic Irrationals, Quadratic Ideals and Indefinite Quadratic Forms

AHMET TEKCAN AND HACER ÖZDEN

Abstract. Let P and Q be two rational integers, $D \neq 1$ be a positive non-square integer, and let $\delta = \sqrt{D}$ or $\frac{1+\sqrt{D}}{2}$ be a real quadratic irrational with trace $t = \delta + \overline{\delta}$ and norm $n = \delta\overline{\delta}$. Given any quadratic irrational $\gamma = \frac{P+\delta}{Q}$, there exist a quadratic ideal $I_\gamma = [Q, \delta + P]$ and an indefinite quadratic form $F_\gamma(x, y) = Qx^2 - (t+2P)xy + \left(\frac{n+tP+P^2}{Q}\right) y^2$ of discriminant $\Delta = t^2 - 4n$ which correspond to γ. In this paper, we obtain some properties of quadratic irrationals γ, quadratic ideals I_γ and indefinite quadratic forms F_γ.

1. Introduction

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

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

with real coefficients a, b, c. The discriminant of F is defined by the formula $b^2 - 4ac$ and is denoted by Δ. Moreover F is an integral form iff $a, b, c \in \mathbb{Z}$ and F is indefinite iff $\Delta > 0$.

Let Γ be the modular group $\mathrm{PSL}(2, \mathbb{Z})$, i.e., the set of the transformations

$$z \mapsto \frac{rz + s}{tz + u}, \quad r, s, t, u \in \mathbb{Z}, \quad ru - st = 1.$$

Γ is generated by the transformations $T(z) = \frac{-1}{z}$ and $V(z) = z + 1$. Let $U = T \cdot V$. Then $U(z) = \frac{-1}{z+1}$. Then Γ has a representation

2000 *Mathematics Subject Classification.* 11E15, 11A55, 11J70.

Key words and phrases. Quadratic irrationals, quadratic ideals, indefinite quadratic forms, extended modular group.

$\Gamma = \langle T, U : T^2 = U^3 = I \rangle$. Note that

$$\Gamma = \left\{ g = \begin{pmatrix} r & s \\ t & u \end{pmatrix} : r, s, t, u \in \mathbb{Z} \text{ and } ru - st = 1 \right\}.$$

We denote the symmetry with respect to the imaginary axis with R, that is $R(z) = -\overline{z}$. Then the group $\overline{\Gamma} = \Gamma \cup R\Gamma$ is generated by the transformations R, T, U and has a representation $\overline{\Gamma} = \langle R, T, U : R^2 = T^2 = U^3 = I \rangle$, and is called the extended modular group. Similarly,

$$\overline{\Gamma} = \left\{ g = \begin{pmatrix} r & s \\ t & u \end{pmatrix} : r, s, t, u \in \mathbb{Z} \text{ and } ru - st = \pm 1 \right\}.$$

There is a strong connection between the extended modular group and binary quadratic forms (for further details see [5]). Most properties of binary quadratic forms can be given by the aid of the extended modular group. The most is equivalence of forms which is given by Gauss as follows: Let $F = (a, b, c)$ be a quadratic form and let $g = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in \overline{\Gamma}$. Then the form gF is defined by

$$\begin{aligned} gF(x, y) = {} & \left(ar^2 + brs + cs^2\right) x^2 + (2art + bru + bts + 2csu)\, xy \\ & + \left(at^2 + btu + cu^2\right) y^2. \end{aligned} \tag{1.1}$$

This definition of gF is a group action of $\overline{\Gamma}$ on the set of binary quadratic forms. Two forms F and G are said to be equivalent iff there exists a $g \in \overline{\Gamma}$ such that $gF = G$. If $\det g = 1$, then F and G are called properly equivalent. If $\det g = -1$, then F and G are called improperly equivalent. A quadratic form F is said to be ambiguous if it is improperly equivalent to itself.

An indefinite quadratic form F of discriminant Δ is said to be reduced if

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

Mollin considers the arithmetic of ideals in his book (see [1]). Let $D \neq 1$ be a square free integer and let $\Delta = \frac{4D}{r^2}$, where

$$r = \begin{cases} 2 & D \equiv 1 \pmod 4 \\ 1 & \text{otherwise}. \end{cases} \tag{1.3}$$

If we set $\mathbb{K} = \mathbb{Q}(\sqrt{D})$, then $\mathbb{K}$ is called a quadratic number field of discriminant $\Delta = \frac{4D}{r^2}$. 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. Therefore $A \cap \mathbb{K} = O_\Delta$ is the ring of integers of the quadratic field $\mathbb{K}$ of discriminant Δ. Set $w_\Delta = \frac{r-1+\sqrt{D}}{r}$ for r defined in (1.3). Then w_Δ is called principal surd. We restate the ring of integers of $\mathbb{K}$ as $O_\Delta = [1, w_\Delta] = \mathbb{Z}[w_\Delta]$. In this case $\{1, w_\Delta\}$ is called an integral basis for $\mathbb{K}$.

$I = [a,\, b + cw_\Delta]$ is a non-zero (quadratic) ideal of O_Δ if and only if

$$c|b,\ c|a \ \text{ and } \ ac|N(b + cw_\Delta). \tag{1.4}$$

Furthermore for a given ideal I the integers a and c are unique and a is the least positive rational integer in I which we will denote as $L(I)$. The norm of an ideal I is defined as $N(I) = |ac|$. If I is an ideal of O_Δ with $L(I) = N(I)$, i.e., $c = 1$, then I is called primitive which means that I has no rational integer factors other than ± 1. Every primitive ideal can be uniquely given by $I = [a, b + w_\Delta]$. The conjugate of an ideal $I = [a,\, b + cw_\Delta]$ is defined as $\overline{I} = [a, \overline{b + cw_\Delta}]$. If $I = \overline{I}$, then I is called ambiguous (see also [4], [2] and [3]).

Let δ denotes a real quadratic irrational integer with trace $t = \delta + \overline{\delta}$ and norm $n = \delta\overline{\delta}$. Thus $\overline{\delta}$ denotes its algebraic conjugate. Evidently 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 by (1.4).

Two real numbers α and β are said to be equivalent if there exists a $g = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in \overline{\Gamma}$ such that $g\alpha = \beta$, that is

$$\frac{r\alpha + s}{t\alpha + u} = \beta. \tag{1.5}$$

Given any quadratic irrational $\gamma = \frac{P+\delta}{Q}$, there exists an indefinite quadratic form

$$\begin{aligned} F_\gamma(x, y) &= Q(x - \delta y)(x - \overline{\delta} y) \\ &= Qx^2 - (t + 2P)xy + \left(\frac{n + Pt + P^2}{Q}\right) y^2 \end{aligned} \tag{1.6}$$

of discriminant $\Delta = t^2 - 4n$. Hence one associates with γ an indefinite quadratic form F_γ defined as above. Therefore if $\delta = \sqrt{D}$, then $t = 0$ and $n = -D$. So $\Delta = 4D$, and if $\delta = \frac{1+\sqrt{D}}{2}$, then $t = 1$ and

$n = \frac{1-D}{4}$. So $\Delta = D$. The connection among γ, I_γ and F_γ is given by the following diagram:

$$\begin{array}{ccc} \gamma = \frac{P+\delta}{Q} & \longrightarrow & I_\gamma = [Q, P+\delta] \\ \downarrow & & \\ F_\gamma(x,y) = Q(x-\delta y)(x-\overline{\delta} y) & & \end{array}$$

The opposite of F_γ defined in (1.6) is

$$\overline{F}_\gamma(x,y) = Qx^2 + (t+2P)xy + \left(\frac{n+Pt+P^2}{Q}\right)y^2 \tag{1.7}$$

of discriminant Δ.

We know that a quadratic form F is said to be ambiguous if it is improperly equivalent to itself. Of course the surprising equivalence must interchange the numbers $\gamma = \frac{\delta+P}{Q}$ and its conjugate $\overline{\gamma} = \frac{\overline{\delta}+P}{Q}$. Thus if all is well the form F_γ is ambiguous iff the number γ is equivalent to its conjugate $\overline{\gamma}$. Therefore one sees that an ideal I_γ is ambiguous if it is equal to its conjugate $\overline{I}_\gamma$. Hence the ideal I_γ is ambiguous iff it contains both $\frac{\delta+P}{Q}$ and $\frac{\overline{\delta}+P}{Q}$ that is so iff

$$\frac{\delta+P}{Q} + \frac{\overline{\delta}+P}{Q} = \frac{t+2P}{Q} \in \mathbb{Z}. \tag{1.8}$$

Therefore the condition $Q|(t+2P)$ is the condition for a form F_γ to be properly equivalent to its opposite $\overline{F}_\gamma$.

2. Quadratic Irrationals, Quadratic Ideals and Indefinite Quadratic Forms

In this section we obtain some properties of quadratic irrationals $\gamma = \frac{\delta+P}{Q}$, quadratic ideals $I_\gamma = [Q, \delta+P]$ and indefinite quadratic forms $F_\gamma(x,y) = Qx^2 - (t+2P)xy + \left(\frac{n+tP+P^2}{Q}\right)y^2$ which are obtained from γ. We consider the problem in two cases: $\delta = \sqrt{D}$ and $\delta = \frac{1+\sqrt{D}}{2}$ for a positive non-square integer D.

First let assume that $\delta = \sqrt{D}$ and $Q = 1$. Then $t = 0$ and $n = -D$. Set $P = \frac{-p}{2}$ for prime p such that $p \equiv 1, 3 \pmod 4$. Then

$$\gamma_1 = \frac{\delta+P}{Q} = \frac{\sqrt{D}+\frac{-p}{2}}{1} = \sqrt{D} - \frac{p}{2}$$

and hence

$$\begin{aligned} I_{\gamma_1} &= \left[1, \sqrt{D} - \frac{p}{2}\right] \\ F_{\gamma_1}(x,y) &= x^2 + pxy + \left(\frac{p^2 - 4D}{4}\right) y^2. \end{aligned}$$

Now we can give some properties of γ_1, I_{γ_1} and F_{γ_1} by the following theorems.

Theorem 2.1. *γ_1 is equivalent to its conjugate $\overline{\gamma}_1$ for every prime $p \equiv 1, 3\ (mod\ 4)$.*

Proof. Recall that $\gamma_1 = \sqrt{D} - \frac{p}{2}$. Then the conjugate of γ_1 is $\overline{\gamma}_1 = -\sqrt{D} - \frac{p}{2}$. A straightforward calculations shows that

$$g\overline{\gamma}_1 = \frac{-1\left(-\sqrt{D} - \frac{p}{2}\right) + (-p)}{0\left(-\sqrt{D} - \frac{p}{2}\right) + 1} = \frac{\sqrt{D} - \frac{p}{2}}{1} = \gamma_1$$

for $g = \begin{pmatrix} -1 & -p \\ 0 & 1 \end{pmatrix} \in \overline{\Gamma}$. Therefore by definition γ_1 is equivalent to its conjugate $\overline{\gamma}_1$. □

Theorem 2.2. *I_{γ_1} is ambiguous for every prime $p \equiv 1, 3\ (mod\ 4)$.*

Proof. We know that an ideal I_γ is ambiguous if it is equal to its conjugate $\overline{I}_\gamma$, or in other words iff $\frac{\delta+P}{Q} + \frac{\overline{\delta}+P}{Q} = \frac{t+2P}{Q} \in \mathbb{Z}$. For $\delta = \sqrt{D}$ we have $t = 0$, and hence $\frac{t+2P}{Q} = \frac{2(-p/2)}{1} = -p \in \mathbb{Z}$. Therefore I_{γ_1} is ambiguous. □

From Theorems 2.1 and 2.2 we can give the following result.

Corollary 2.3. *F_{γ_1} is properly equivalent to its opposite $\overline{F}_{\gamma_1}$ and is ambiguous for every prime $p \equiv 1, 3\ (mod\ 4)$.*

Proof. It is clear that F_{γ_1} is properly equivalent to its opposite $\overline{F}_{\gamma_1}$ by (1.8) since $\frac{t+2P}{Q} = -p \in \mathbb{Z}$. We know as above that an indefinite quadratic form F_γ is ambiguous iff the quadratic irrational γ is equivalent to its conjugate $\overline{\gamma}$. Therefore F_{γ_1} is ambiguous since γ_1 is equivalent to its conjugate $\overline{\gamma}_1$ by Theorem 2.1. □

Now let $p \equiv 1, 3$ (mod 4), i.e., $p = 1+4k$ or $p = 3+4k$ for a positive integer k, respectively. Then we have the following theorem.

Theorem 2.4. *If F_{γ_1} is reduced, then*

$$D \in [4k^2 + 2k + 1,\, 4k^2 + 6k + 2] - \{4k^2 + 4k + 1\}$$

for $p \equiv 1 \ (mod\ 4)$, and if F_{γ_1} is reduced, then

$$D \in [4k^2 + 6k + 3,\, 4k^2 + 10k + 6] - \{4k^2 + 8k + 4\}$$

for $p \equiv 3 \ (mod\ 4)$. In both cases the number of these reduced forms is p.

Proof. Let $F_{\gamma_1}(x, y) = x^2 + pxy + \left(\frac{p^2-4D}{4}\right) y^2$ be reduced and let $p \equiv 1 \pmod 4$. Then by definition, we have from (1.2)

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

$$\Longleftrightarrow \left|\sqrt{4D} - 2|1|\right| < p < \sqrt{4D} \Leftrightarrow 2|\sqrt{D} - 1| < p < 2\sqrt{D}.$$

Hence we get $D \geq 4k^2 + 2k + 1$, since

$$D > \frac{p^2}{4} = \frac{(1 + 4k)^2}{4} = \frac{1 + 8k + 16k^2}{4} = \frac{1}{4} + 2k + 4k^2$$

and $D \leq 4k^2 + 6k + 2$, since

$$D < \frac{(p + 2)^2}{4} = \frac{(3 + 4k)^2}{4} = \frac{9 + 24k + 16k^2}{4} = \frac{9}{4} + 6k + 4k^2.$$

Consequently we have

$$4k^2 + 2k + 1 \leq D \leq 4k^2 + 6k + 2.$$

Note that there exist $p + 1$ indefinite reduced quadratic forms F_{γ_1}, since

$$4k^2 + 6k + 2 - \left(4k^2 + 2k + 1\right) + 1 = 2 + 4k = p + 1.$$

But $D = 4k^2 + 4k + 1 = \left(\frac{p+1}{2}\right)^2 \in [4k^2 + 2k + 1,\, 4k^2 + 6k + 2]$ is a square. So we have to omit it (D must be a square-free positive integer). Therefore there exist p indefinite reduced quadratic forms F_{γ_1} for $D \in [4k^2 + 2k + 1,\, 4k^2 + 6k + 2] - \{4k^2 + 4k + 1\}$.

Similarly, let $F_{\gamma_1}(x, y) = x^2 + pxy + \left(\frac{p^2-4D}{4}\right) y^2$ be reduced and let $p \equiv 3 \pmod 4$. Then by definition, we have from (1.2)

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

$$\Longleftrightarrow \left|\sqrt{4D} - 2|1|\right| < p < \sqrt{4D} \Leftrightarrow 2|\sqrt{D} - 1| < p < 2\sqrt{D}.$$

Hence we get $D \geq 4k^2 + 6k + 3$, since

$$D > \frac{p^2}{4} = \frac{(3+4k)^2}{4} = \frac{9+24k+16k^2}{4} = \frac{9}{4} + 6k + 4k^2$$

and $D \leq 4k^2 + 10k + 6$, since

$$D < \frac{(p+2)^2}{4} = \frac{(5+4k)^2}{4} = \frac{25+40k+16k^2}{4} = \frac{25}{4} + 10k + 4k^2.$$

Consequently we have

$$4k^2 + 6k + 3 \leq D \leq 4k^2 + 10k + 6.$$

Note that there exist $p+1$ indefinite reduced quadratic forms F_{γ_1}, since

$$4k^2 + 10k + 6 - \big(4k^2 + 6k + 3\big) + 1 = 4k + 4 = p + 1.$$

But $D = 4k^2 + 8k + 4 = \left(\frac{p+1}{2}\right)^2 \in [4k^2 + 6k + 3,\, 4k^2 + 10k + 6]$ is a square. So we have to omit it. Therefore there exist p indefinite reduced quadratic forms F_{γ_1} for $D \in [4k^2 + 6k + 3,\, 4k^2 + 10k + 6] - \{4k^2 + 8k + 4\}$. □

Example 2.1. Let $p = 29 \equiv 1 \pmod 4$. Then $\gamma_1 = \sqrt{D} - \frac{29}{2}$ is equivalent to its conjugate $\overline{\gamma}_1$ for $g = \begin{pmatrix} -1 & -29 \\ 0 & 1 \end{pmatrix} \in \overline{\Gamma}$. Also $I_{\gamma_1} = \left[1, \sqrt{D} - \frac{29}{2}\right]$ is ambiguous, and

$$F_{\gamma_1}(x,y) = x^2 + 29xy + \left(\frac{841 - 4D}{4}\right) y^2$$

is reduced for $D \in [211, 240]$. But $D = 225 = 15^2 \in [211, 240]$ is a square. Therefore F_{γ_1} is reduced for $D \in [211, 240] - \{225\}$. The number of these reduced forms is 29. Further F_{γ_1} is properly equivalent to its opposite $\overline{F}_{\gamma_1}$ and is ambiguous.

Example 2.2. Let $p = 43 \equiv 3 \pmod 4$. Then $\gamma_1 = \sqrt{D} - \frac{43}{2}$ is equivalent to its conjugate $\overline{\gamma}_1$ for $g = \begin{pmatrix} -1 & -43 \\ 0 & 1 \end{pmatrix} \in \overline{\Gamma}$. Also $I_{\gamma_1} = \left[1, \sqrt{D} - \frac{43}{2}\right]$ is ambiguous, and

$$F_{\gamma_1}(x,y) = x^2 + 43xy + \left(\frac{1849 - 4D}{4}\right) y^2$$

is reduced for $D \in [421, 462]$. But $D = 441 = 21^2 \in [421, 462]$ is a square. Therefore F_{γ_1} is reduced for $D \in [421, 462] - \{441\}$.

The number of these reduced forms is 43. Further F_{γ_1} is properly equivalent to its opposite $\overline{F}_{\gamma_1}$ and is ambiguous.

Now we consider the case $\delta = \frac{1+\sqrt{D}}{2}$ and $Q = 1$. Then $t = 1$ and $n = \frac{1-D}{4}$. Set $P = \frac{-(p+1)}{2}$ for prime p such that $p \equiv 1, 3 \pmod 4$. Then

$$\gamma_2 = \frac{P+\delta}{Q} = \frac{\frac{-(p+1)}{2} + \frac{1+\sqrt{D}}{2}}{1} = \frac{-p+\sqrt{D}}{2}$$

and hence

$$\begin{aligned} I_{\gamma_2} &= \left[1, \frac{-p+\sqrt{D}}{2}\right] \\ F_{\gamma_2}(x,y) &= x^2 + pxy + \left(\frac{p^2-D}{4}\right)y^2. \end{aligned}$$

Theorem 2.5. *γ_2 is equivalent to its conjugate $\overline{\gamma}_2$ for every prime $p \equiv 1, 3$ $(mod\ 4)$.*

Proof. Recall that $\gamma_2 = \frac{-p+\sqrt{D}}{2}$. The conjugate of γ_2 is $\overline{\gamma}_2 = \frac{-p-\sqrt{D}}{2}$. Applying (1.5), we get

$$g\overline{\gamma}_2 = \frac{-1\left(\frac{-p-\sqrt{D}}{2}\right) + (-p)}{0\left(\frac{-p-\sqrt{D}}{2}\right) + 1} = \frac{-p+\sqrt{D}}{2} = \gamma_2$$

for $g = \begin{pmatrix} -1 & -p \\ 0 & 1 \end{pmatrix} \in \overline{\Gamma}$. Therefore by definition γ_2 is equivalent to its conjugate $\overline{\gamma}_2$. □

Theorem 2.6. *I_{γ_2} is ambiguous for every prime $p \equiv 1, 3$ $(mod\ 4)$.*

Proof. We know that an ideal I_γ is ambiguous if it is equal to its conjugate $\overline{I}_\gamma$, or in other words iff $\frac{\delta+P}{Q} + \frac{\overline{\delta}+P}{Q} = \frac{t+2P}{Q} \in \mathbb{Z}$. For $\delta = \frac{1+\sqrt{D}}{2}$ we have $t = 1$, and hence $\frac{t+2P}{Q} = \frac{1+2((-p-1)/2)}{1} = -p \in \mathbb{Z}$. Therefore I_{γ_2} is ambiguous. □

From Theorems 2.5 and 2.6 we can give the following corollary.

Corollary 2.7. *F_{γ_2} is properly equivalent to its opposite $\overline{F}_{\gamma_2}$ and is ambiguous for every prime $p \equiv 1, 3$ $(mod\ 4)$.*

Proof. It is clear that F_{γ_2} is properly equivalent to its opposite $\overline{F}_{\gamma_2}$ by (1.8) since $\frac{t+2P}{Q} = -p \in \mathbb{Z}$, and is ambiguous since γ_2 is equivalent to its conjugate $\overline{\gamma}_2$ by Theorem 2.5. □

Theorem 2.8. *If F_{γ_2} is reduced, then*

$$D \in [16k^2 + 8k + 2,\ 16k^2 + 24k + 8] - \{16k^2 + 16k + 4\}$$

for $p \equiv 1\ (mod\ 4)$, and if F_{γ_2} is reduced, then

$$D \in [16k^2 + 24k + 10, 16k^2 + 40k + 24] - \{16k^2 + 32k + 16\}$$

for $p \equiv 3\ (mod\ 4)$. In both cases the number of these forms is $4p+2$.

Proof. Let $F_{\gamma_2}(x, y) = x^2 + pxy + \left(\frac{p^2-D}{4}\right) y^2$ be reduced and let $p \equiv 1 \pmod 4$. Then by definition we have from (1.2),

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

$$\iff \left|\sqrt{D} - 2|1|\right| < p < \sqrt{D} \Leftrightarrow \left|\sqrt{D} - 2\right| < p < \sqrt{D}.$$

Hence we get $D \geq 16k^2 + 8k + 2$, since

$$D > p^2 = (1 + 4k)^2 = 1 + 8k + 16k^2$$

and $D \leq 16k^2 + 24k + 8$, since

$$D < (p + 2)^2 = (3 + 4k)^2 = 9 + 24k + 16k^2.$$

Consequently we have

$$16k^2 + 8k + 2 \leq D \leq 16k^2 + 24k + 8.$$

Note that there exist $4p + 3$ indefinite reduced quadratic forms F_{γ_2}, since

$$16k^2+24k+8-\left(16k^2 + 8k + 2\right)+1 = 16k+7 = 4(1+4k)+3 = 4p+3.$$

But $D = 16k^2+16k+4 = (p+1)^2 \in [16k^2+8k+2,\ 16k^2+24k+8]$ is a square. So we have to omit it. Therefore there exist $4p+2$ indefinite reduced quadratic forms F_{γ_2} for $D \in [16k^2 + 8k + 2,\ 16k^2 + 24k + 8] - \{16k^2 + 16k + 4\}$.

Similarly, let $F_{\gamma_2}(x, y) = x^2 + pxy + \left(\frac{p^2-D}{4}\right) y^2$ be reduced and let $p \equiv 3 \pmod 4$. Then by definition we have from (1.2),

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

$$\iff \left|\sqrt{D} - 2|1|\right| < p < \sqrt{D} \Leftrightarrow \left|\sqrt{D} - 2\right| < p < \sqrt{D}.$$

Hence we get $D \geq 16k^2 + 24k + 10$, since

$$D > p^2 = (3 + 4k)^2 = 9 + 24k + 16k^2$$

and $D \leq 16k^2 + 40k + 24$, since

$$D < (p + 2)^2 = (5 + 4k)^2 = 25 + 40k + 16k^2.$$

Consequently, we have

$$16k^2 + 24k + 10 \leq D \leq 16k^2 + 40k + 24.$$

Note that there exist $4p + 3$ indefinite reduced quadratic forms F_{γ_2}, since

$$\begin{aligned} 16k^2 + 40k + 24 - \big(16k^2 + 24k + 10\big) + 1 \\ = 16k + 15 = 4(3 + 4k) + 3 = 4p + 3. \end{aligned}$$

But $D = 16k^2 + 32k + 16 = (p + 1)^2 \in [16k^2 + 24k + 10, 16k^2 + 40k + 24]$ is a square. So we have to omit it. Therefore there exist $4p + 2$ indefinite reduced quadratic forms F_{γ_2} for $D \in [16k^2 + 24k + 10, 16k^2 + 40k + 24] - \{16k^2 + 32k + 16\}$. □

Example 2.3. Let $p = 73 \equiv 1 \pmod 4$. Then $\gamma_2 = \frac{-73+\sqrt{D}}{2}$ is equivalent to its conjugate $\overline{\gamma}_2$ for $g = \begin{pmatrix} -1 & -73 \\ 0 & 1 \end{pmatrix} \in \overline{\Gamma}$. Also $I_{\gamma_2} = \left[1, \frac{-73+\sqrt{D}}{2}\right]$ is ambiguous, and

$$F_{\gamma_2}(x, y) = x^2 + 73xy + \left(\frac{5329 - D}{4}\right) y^2$$

is reduced for $D \in [5330, 5624]$. But $D = 5476 = 74^2 \in [5330, 5624]$ is a square. Therefore F_{γ_2} is reduced for $D \in [5330, 5624] - \{5476\}$. The number of these reduced forms is 294. Further F_{γ_2} is properly equivalent to its opposite $\overline{F}_{\gamma_2}$ and is ambiguous.

Example 2.4. Let $p = 83 \equiv 3 \pmod 4$. Then $\gamma_2 = \frac{-83+\sqrt{D}}{2}$ is equivalent to its conjugate $\overline{\gamma}_2$ for $g = \begin{pmatrix} -1 & -83 \\ 0 & 1 \end{pmatrix} \in \overline{\Gamma}$. Also $I_{\gamma_2} = \left[1, \frac{-83+\sqrt{D}}{2}\right]$ is ambiguous, and

$$F_{\gamma_2}(x, y) = x^2 + 83xy + \left(\frac{6889 - D}{4}\right) y^2$$

is reduced for $D \in [6890, 7224]$. But $D = 7056 = 84^2 \in [6890, 7224]$ is a square. Therefore F_{γ_2} is reduced for $D \in [6890, 7224] - \{7056\}$.

The number of these reduced forms is 334. Further F_{γ_2} is properly equivalent to its opposite $\overline{F}_{\gamma_2}$ and is ambiguous.

References

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

[2] R. A. Mollin, *Jocabi symbols, ambiguous ideals, and continued fractions*, Acta Arith. **85** (1998), 331–349.

[3] R. A. Mollin, *A survey of Jacobi symbols, ideals, and continued fractions*, Far East J. Math. Sci. **6** (1998), 355–368.

[4] R. A. Mollin, K. Cheng, *Palindromy and ambiguous ideals revisited*, J. Number Theory **74** (1999), 98–110.

[5] A. Tekcan, O. Bizim, *The connection between quadratic forms and the extended modular group*, Mathematica Bohemica **128**(3) (2003), 225–236.

Ahmet Tekcan and Hacer Özden,
Department of Mathematics,
Faculty of Science,
Uludag University,
Görükle 16059,
Bursa, Turkey
tekcan@uludag.edu.tr; hozden@uludag.edu.tr

Received on 9 March 2006 and in revised form on 1 September 2006.