INDEFINITE QUADRATIC FORMS AND PELL EQUATIONS INVOLVING QUADRATIC IDEALS

AHMET TEKCAN

Communicated by Alexandru Zaharescu

Let $p \equiv 1 (\text{mod } 4)$ be a prime number, let $\gamma = \frac{P+\sqrt{p}}{Q}$ be a quadratic irrational, let $I_\gamma = [Q, P + \sqrt{p}]$ be a quadratic ideal and let $F_\gamma = (Q, 2P, -Q)$ be an indefinite quadratic form of discriminant $\Delta = 4p$, where P and Q are positive integers depending on p. In this work, we first determined the cycle of I_γ and then proved that the right and left neighbors of F_γ can be obtained from the cycle of I_γ. Later we determined the continued fraction expansion of γ, and then we showed that the continued fraction expansion of $\sqrt{p}$, the set of proper automorphisms of F_γ, the fundamental solution of the Pell equation $x^2 - py^2 = \pm 1$ and the set of all positive integer solutions of the equation $x^2 - py^2 = \pm p$ can be obtained from the continued fraction expansion of γ.

AMS 2010 Subject Classification: 11E08, 11E10, 11E16, 11D09, 11D41, 11D45.

Key words: quadratic irrationals, quadratic ideals, quadratic forms, cycles, right and left neighbors, proper automorphisms, Pell equation.

1. INTRODUCTION

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 $\Delta = \Delta(F)$. 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 $|\sqrt{\Delta} - 2|a|| < b < \sqrt{\Delta}$.

Gauss defined the **group action** of GL(2,$\mathbb{Z}$) which is the multiplicative group of 2×2 matrices $g = \begin{bmatrix} r & s \\ t & u \end{bmatrix}$ such that $r, s, t, u \in \mathbb{Z}$ with $\det(g) = \pm 1$ on the set of forms as

$$gF(x, y) = F(rx + ty, sx + uy) \tag{1.1}$$

for $g = \begin{bmatrix} r & s \\ t & u \end{bmatrix} \in$GL$(2,\mathbb{Z})$. If there exists a $g \in$GL$(2,\mathbb{Z})$ 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**. An element $g \in$GL$(2,\mathbb{Z})$ 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 $Aut(F)^+$ denote the set of proper automorphisms and let $Aut(F)^-$ denote the set of improper automorphisms of F.

The **right neighbor** $R(F)$ of an integral indefinite form $F = (a, b, c)$ of discriminant Δ is the form (A, B, C) determined by four conditions:

$$A = c, b + B \equiv 0 \pmod{2A}, \sqrt{\Delta} - 2|A| < B < \sqrt{\Delta} \text{ and } B^2 - 4AC = \Delta.$$

It is clear that

$$R(F) = \begin{bmatrix} 0 & -1 \\ 1 & -\delta \end{bmatrix} (a, b, c), \tag{1.2}$$

where

$$\delta = \frac{b + B}{2c}. \tag{1.3}$$

The **left neighbor** $L(F)$ of F is defined as

$$L(F) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} R(c, b, a). \tag{1.4}$$

So F is properly equivalent to its right and left neighbor.

Let $\rho(F)$ denote the normalization of $(c, -b, a)$. Let $F = F_0 = (a_0, b_0, c_0)$ and let $r_i = sign(c_i)\left\lfloor \frac{b_i}{2|c_i|} \right\rfloor$ for $|c_i| \geq \sqrt{\Delta}$ or $r_i = sign(c_i)\left\lfloor \frac{b_i + \sqrt{\Delta}}{2|c_i|} \right\rfloor$ for $|c_i| < \sqrt{\Delta}$ with $i \geq 0$. Then the **reduction** of F is $\rho^{i+1}(F) = (c_i, -b_i + 2c_i r_i, c_i r_i^2 - b_i r_i + a_i)$. Then the **proper cycle** of F is the sequence $(\rho^i(G))$ for $i \in \mathbb{Z}$, where G is a reduced form which is properly equivalent to F and the **cycle** of F is the sequence $((\tau\rho)^i(G))$ for $i \in \mathbb{Z}$, where $G = (A, B, C)$ is a reduced form with $A > 0$ which is equivalent to F for $\tau(F) = (-a, b, -c)$. The cycle of a reduced integral form F is computed as follows: Let $F_0 = F$, $s_i = \left\lfloor \frac{b_i + \sqrt{\Delta}}{2|c_i|} \right\rfloor$ and let

$$F_{i+1} = \left(|c_i|, -b_i + 2s_i|c_i|, -a_i - b_i s_i - c_i s_i^2\right).$$

Then the cycle of F is $F_0 \sim F_1 \sim F_2 \sim \cdots \sim F_{l-1}$ of length l. If l is odd, then the proper cycle of F is $F_0 \sim \tau(F_1) \sim F_2 \sim \tau(F_3) \sim \cdots \sim \tau(F_{l-2}) \sim F_{l-1} \sim \tau(F_0) \sim F_1 \sim \tau(F_2) \sim \cdots \sim F_{l-2} \sim \tau(F_{l-1})$ of length $2l$ and if l is even, then the proper cycle of F is $F_0 \sim \tau(F_1) \sim F_2 \sim \tau(F_3) \sim \cdots \sim F_{l-2} \sim \tau(F_{l-1})$ of length l (for further details see [2–4]).

Mollin considered the arithmetic of ideals in his book [6]. Let $D \neq 1$ be a square–free integer and let $\Delta = \frac{4D}{r^2}$, where $r = 2$ if $D \equiv 1 (\bmod 4)$ or $r = 1$ otherwise. Then Δ is called a **fundamental discriminant** with fundamental radicand D. If we set $\mathbb{K} = \mathbb{Q}(\sqrt{D})$, then $\mathbb{K}$ is called a **real quadratic number field** of discriminant Δ. Thus, there is 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. Therefore $A \cap \mathbb{K} = O_\Delta$ is the ring of integers of the quadratic field $\mathbb{K}$ of discriminant Δ.

A real number γ is called a **quadratic irrational** associated with the radicand D, if γ can be written as $\gamma = \frac{P+\sqrt{D}}{Q}$, where $P, Q, D \in \mathbb{Z}$, $D > 0, Q \neq 0$ and $P^2 \equiv D (\bmod Q)$. We denote the **continued fraction expansion** of γ by $\gamma = [m_0; m_1, m_2, \cdots, \gamma_i]$, where (for $i \geq 0$ and $\gamma = \gamma_0, P_0 = P, Q_0 = Q$) we recursively define $\gamma_i = \frac{P_i+\sqrt{D}}{Q_i}$,

$$(1.5) \qquad m_i = \left\lfloor \frac{P_i + \sqrt{D}}{Q_i} \right\rfloor, \ P_{i+1} = m_i Q_i - P_i \ \text{ and } \ Q_{i+1} = \frac{D - P_{i+1}^2}{Q_i}.$$

An infinite simple continued fraction γ is called **periodic** if $\gamma = [m_0; m_1, m_2, \cdots]$, where $m_n = m_{n+l}$ for all $n \geq k$ with $k, l \in \mathbb{N}$. In this case we use the notation $[m_0; m_1, m_2, \cdots, m_{k-1}; \overline{m_k, m_{k+1}, \cdots, m_{l+k-1}}]$. An infinite simple continued fraction γ is called **purely periodic** if $\gamma = [\overline{m_0; m_1, \cdots, m_{l-1}}]$ with **period length** l. If γ is a quadratic irrational, then $I_\gamma = [Q, P + \sqrt{D}]$ is a quadratic ideal and its cycle is $I_{\gamma_0} \sim I_{\gamma_1} \sim \cdots \sim I_{\gamma_{l-1}}$ of length l.

In [8], Mollin considered the Jocabi symbols, ambiguous ideals and continued fractions. In [9], Mollin and Cheng derived some results on palindromy and ambiguous ideals. In [10], we considered the proper cycles of a reduced form F and its right neighbors. We proved that the proper cycle of a reduced form F can be given by its consecutive right neighbors, namely,

Lemma 1.1 ([10, Theorem 2.1]). *Let $F_0 \sim F_1 \sim \cdots \sim F_{l-1}$ be the cycle of a reduced form F of length l, and let $R^i(F_0)$ be the consecutive right neighbors of $F = F_0$ for $i \geq 0$. Then*

(1) *If l is odd, then the proper cycle of F is $F_0 \sim R^1(F_0) \sim \cdots \sim R^{2l-2}(F_0) \sim R^{2l-1}(F_0)$ of length $2l$.*
(2) *If l is even, then the proper cycle of F is $F_0 \sim R^1(F_0) \sim \cdots \sim R^{l-2}(F_0) \sim R^{l-1}(F_0)$ of length l.*

Later in [11], the present author and collaborators considered the same problem for the left neighbors and proved that

Lemma 1.2 (11, Theorem 4). *Let $F_0 \sim F_1 \sim \cdots \sim F_{l-1}$ be the cycle of a reduced form F of length l, and let $L^i(F_0)$ be the consecutive left neighbors of $F = F_0$ for $i \geq 0$. Then*

(1) *If l is odd, then the proper cycle of F is $F_0 \sim L^{2l-1}(F_0) \sim \cdots \sim L^2(F_0) \sim L^1(F_0)$ of length $2l$.*
(2) *If l is even, then the proper cycle of F is $F_0 \sim L^{l-1}(F_0) \sim \cdots \sim L^2(F_0) \sim L^1(F_0)$ of length l.*

Now let p be a prime number such that $p \equiv 1 (\text{mod } 4)$. Let $\gamma = \frac{P+\sqrt{p}}{Q}$ be a quadratic irrational, let $I_\gamma = [Q, P + \sqrt{p}]$ be a quadratic ideal and let $F_\gamma = (Q, 2P, -Q)$ be an indefinite quadratic form of discriminant $\Delta = 4p$ for some positive integers P and Q depending on p. In the present paper, we demonstrate

(1) how to use the cycle of I_γ to determine the left and right neighbors of F_γ.
(2) how to use the continued fraction expansion of γ to determine
   - the continued fraction expansion of $\sqrt{p}$,
   - the set of proper automorphisms of F_γ,
   - the fundamental solution of the Pell equation $x^2 - py^2 = \pm 1$,
   - the set of all positive integer solutions of the equation $x^2 - py^2 = \pm p$.

Recall that the equation

$$x^2 - dy^2 = \pm n \tag{1.6}$$

is called a **norm–form equation** since $N(x + y\sqrt{d}) = x^2 - dy^2$ is called the **norm** of $x + y\sqrt{d}$, where d is any positive non–square integer and n is any fixed integer. When $n = 1$, (1.6) is known as the **Pell equation** after John Pell (1611–1685), who actually had little to do with its solution. The Pell equation $x^2 - dy^2 = \pm 1$ has infinitely many integer solutions. (In particular, $x^2 - dy^2 = -1$ has infinitely many solutions when the length of the continued fraction expansion of $\sqrt{d}$ is odd). The first non–trivial positive integer solutions (x_1, y_1) is called the **fundamental solution** from which all integer solutions can be derived. Namely, if (x_1, y_1) is the fundamental solution of $x^2 - dy^2 = 1$, then the other solutions are (x_n, y_n), where $x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n$ for $n \geq 1$ and if (x_1, y_1) is the fundamental solution of $x^2 - dy^2 = -1$, then the other solutions are (x_{2n+1}, y_{2n+1}), where $x_{2n+1} + y_{2n+1}\sqrt{d} = (x_1 + y_1\sqrt{d})^{2n+1}$ for $n \geq 0$ (see [1, 5, 7]).

Let $\alpha = [q_0; q_1, \cdots, q_l]$ for $l \in \mathbb{N}$ be a finite continued fraction expansion. Define two sequences $A_{-2} = 0, A_{-1} = 1, A_k = q_k A_{k-1} + A_{k-2}$ and $B_{-2} = 1, B_{-1} = 0, B_k = q_k\ B_{k-1} + B_{k-2}$ for a nonnegative integer k. Then $C_k =$

$\frac{A_k}{B_k}$ is the k^{th} convergent of α for any nonnegative integer $k \leq l$. Then the fundamental solution is given below.

LEMMA 1.3 ([7, Corollary 5.7]). *If $D > 0$ is not a perfect square and $\sqrt{D}$ has continued fraction expansion of period length l, then the fundamental solution of $x^2 - Dy^2 = 1$ is given by $(x_1, y_1) = (A_{l-1}, B_{l-1})$ if l is even or (A_{2l-1}, B_{2l-1}) if l is odd. If l is odd, then the fundamental solution of $x^2 - Dy^2 = -1$ is given by $(x_1, y_1) = (A_{l-1}, B_{l-1})$.*

2. MAIN RESULTS

Let p be a prime number such that $p \equiv 1 (\bmod 4)$. Then it is known that p can be written of the form $p = a^2 + b^2$, where a is odd, b is even and $a + b \equiv 1 (\bmod 4)$. Now we set

$$P = b, Q = |a| \text{ and } D = p. \tag{2.1}$$

Then

$$\gamma = \frac{P + \sqrt{p}}{Q} \tag{2.2}$$

is a quadratic irrational since $P^2 \equiv p \,(\bmod\, Q)$, and so

$$I_\gamma = [Q, P + \sqrt{p}] \tag{2.3}$$

is a quadratic ideal and

$$F_\gamma(x, y) = Q(x + \gamma y)(x + \overline{\gamma} y) = Qx^2 + 2Pxy - Qy^2 \tag{2.4}$$

is an indefinite quadratic form of discriminant $\Delta = 4p$. Here we note that for some values of p, we have $Q = 1$; but for some values of p, we have $Q \neq 1$. (For instance, for $p = 13$, we have $P = 2, Q = 3$, but for $p = 17$, we have $P = 4, Q = 1$). Therefore, we will consider all results in two cases: $Q \neq 1$ or $Q = 1$.

THEOREM 2.1. *Let I_γ be the ideal in (2.3).*

(1) If $Q \neq 1$, then the cycle of I_γ is

$$\begin{aligned} &I_{\gamma_0} = [Q_0, P_0 + \sqrt{p}] \sim I_{\gamma_1} = [Q_1, P_1 + \sqrt{p}] \sim I_{\gamma_2} = [Q_2, P_2 + \sqrt{p}] \sim \cdots \sim \\ &I_{\gamma_{\frac{l-3}{2}}} = [Q_{\frac{l-3}{2}}, P_{\frac{l-3}{2}} + \sqrt{p}] \sim I_{\gamma_{\frac{l-1}{2}}} = [Q_{\frac{l-1}{2}}, P_{\frac{l-1}{2}} + \sqrt{p}] \sim \\ &I_{\gamma_{\frac{l+1}{2}}} = [Q_{\frac{l-3}{2}}, P_{\frac{l-1}{2}} + \sqrt{p}] \sim I_{\gamma_{\frac{l+3}{2}}} = [Q_{\frac{l-5}{2}}, P_{\frac{l-3}{2}} + \sqrt{p}] \sim \cdots \sim \\ &I_{\gamma_{l-2}} = [Q_1, P_2 + \sqrt{p}] \sim I_{\gamma_{l-1}} = [Q_0, P_1 + \sqrt{p}] \end{aligned}$$

of length l.

(2) If $Q = 1$, then the cycle of I_γ is $I_{\gamma_0} = [1, P_0 + \sqrt{p}]$ of length 1.

Proof. (1) Let $Q \neq 1$. Then from (1.5), we deduce the values in Table 1.

TABLE 1

Cycle of I_γ

i	0	1	$\cdots$	$\frac{l-3}{2}$	$\frac{l-1}{2}$	$\frac{l+1}{2}$	$\frac{l+3}{2}$	$\cdots$	$l-2$	$l-1$
P_i	P_0	P_1	$\cdots$	$P_{\frac{l-3}{2}}$	$P_{\frac{l-1}{2}}$	$P_{\frac{l-1}{2}}$	$P_{\frac{l-3}{2}}$	$\cdots$	P_2	P_1
Q_i	Q_0	Q_1	$\cdots$	$Q_{\frac{l-3}{2}}$	$Q_{\frac{l-1}{2}}$	$Q_{\frac{l-3}{2}}$	$Q_{\frac{l-5}{2}}$	$\cdots$	Q_1	Q_0
m_i	m_0	m_1	$\cdots$	$m_{\frac{l-3}{2}}$	$m_{\frac{l-1}{2}}$	$m_{\frac{l-3}{2}}$	$m_{\frac{l-5}{2}}$	$\cdots$	m_1	m_0

So the the cycle of I_γ is

$$\begin{aligned}&I_{\gamma_0} = [Q_0, P_0 + \sqrt{p}] \sim I_{\gamma_1} = [Q_1, P_1 + \sqrt{p}] \sim I_{\gamma_2} = [Q_2, P_2 + \sqrt{p}] \sim \cdots \sim \\ &I_{\gamma_{\frac{l-3}{2}}} = [Q_{\frac{l-3}{2}}, P_{\frac{l-3}{2}} + \sqrt{p}] \sim I_{\gamma_{\frac{l-1}{2}}} = [Q_{\frac{l-1}{2}}, P_{\frac{l-1}{2}} + \sqrt{p}] \sim \\ &I_{\gamma_{\frac{l+1}{2}}} = [Q_{\frac{l-3}{2}}, P_{\frac{l-1}{2}} + \sqrt{p}] \sim I_{\gamma_{\frac{l+3}{2}}} = [Q_{\frac{l-5}{2}}, P_{\frac{l-3}{2}} + \sqrt{p}] \sim \cdots \sim \\ &I_{\gamma_{l-2}} = [Q_1, P_2 + \sqrt{p}] \sim I_{\gamma_{l-1}} = [Q_0, P_1 + \sqrt{p}]\end{aligned}$$

of length l.

(2) Let $Q = 1$. Then from (1.5), we get $m_0 = 2P$ and hence $P_1 = P = P_0$ and $Q_1 = 1 = Q_0$. So the cycle of I_γ is $I_{\gamma_0} = [1, P_0 + \sqrt{p}]$ of length 1. □

Note that in Lemma 1.1, we proved that the proper cycle of a reduced form F can be given by its consecutive right neighbors and in Lemma 1.2, we showed that the proper cycle of a reduced form F can be given by its consecutive left neighbors. Now by virtue of Theorem 2.1, we show that the right and left neighbors of F_γ can be obtained from the cycle of I_γ as follows.

THEOREM 2.2. *Let $I_\gamma = I_{\gamma_0} \sim I_{\gamma_1} \sim \cdots \sim I_{\gamma_{l-1}}$ be the cycle of I_γ of length l.*

(1) *If $Q \neq 1$, then the right neighbors of F_γ in (2.4) are*

$$R^1(F_\gamma), R^2(F_\gamma), \cdots, R^{l-1}(F_\gamma), R^l(F_\gamma), R^{l+1}(F_\gamma), \cdots, R^{2l-1}(F_\gamma),$$

where

$$\begin{aligned}R^i(F_\gamma) &= ((-1)^{i+2}Q_{i-1}, 2P_i, (-1)^{i+1}Q_i) \ for\ 1 \leq i \leq l-1 \\ R^l(F_\gamma) &= (-Q_0, 2P_0, Q_0) \\ R^{l+i}(F_\gamma) &= ((-1)^{i+1}Q_{i-1}, 2P_i, (-1)^{i+2}Q_i) \ for\ 1 \leq i \leq l-1\end{aligned}$$

and the left neighbors of F_γ are

$$L^1(F_\gamma), L^2(F_\gamma), \cdots, L^{l-1}(F_\gamma), L^l(F_\gamma), L^{l+1}(F_\gamma), \cdots, L^{2l-1}(F_\gamma),$$

where

$$\begin{aligned} L^i(F_\gamma) &= ((-1)^{i+2}Q_i, 2P_i, (-1)^{i+1}Q_{i-1}) \ for \ 1 \leq i \leq l-1 \\ L^l(F_\gamma) &= (-Q_0, 2P_0, Q_0) \\ L^{l+i}(F_\gamma) &= ((-1)^{i+1}Q_i, 2P_i, (-1)^{i+2}Q_{i-1}) \ for \ 1 \leq i \leq l-1. \end{aligned}$$

(2) *If* $Q = 1$, *then* F_γ *has one right and one left neighbor and they are same, that is* $R^1(F_\gamma) = L^1(F_\gamma) = (-1, 2P, 1)$.

Proof. (1) Let $Q \neq 1$ and let $F_\gamma = F_{\gamma 0} = (Q_0, 2P_0, -Q_0)$. Then for the first right neighbor $R^1(F_\gamma) = (A, B, C)$, we have $A = -Q_0$. Also $B + 2P_0 \equiv 0 (\text{mod } Q_0)$ is satisfied for $B = 2P_1$ in the range $\sqrt{4(P_0^2 + Q_0^2)} - 2Q_0 < B < \sqrt{4(P_0^2 + Q_0^2)}$ and hence $C = Q_1$, that is, $R^1(F_\gamma) = (-Q_0, 2P_1, Q_1)$. Similarly, we get

$$\begin{aligned} & R^2(F_\gamma) = (Q_1, 2P_2, -Q_2), R^3(F_\gamma) = (-Q_2, 2P_3, Q_3), \cdots, \\ & R^{l-1}(F_\gamma) = (Q_{l-2}, 2P_{l-1}, -Q_{l-1}), R^l(F_\gamma) = (-Q_0, 2P_0, Q_0), \\ & R^{l+1}(F_\gamma) = (Q_0, 2P_1, -Q_1), \cdots, R^{2l-1}(F_\gamma) = (-Q_{l-2}, 2P_{l-1}, Q_{l-1}), \\ & R^{2l}(F_\gamma) = (Q_0, 2P_0, -Q_0) = F_\gamma. \end{aligned}$$

Applying (1.4), the first left neighbor of F_γ is

$$L^1(F_\gamma) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} R(-Q_0, 2P_0, Q_0) = (-Q_1, 2P_1, Q_0).$$

Similarly, we find that

$$\begin{aligned} & L^2(F_\gamma) = (Q_2, 2P_2, -Q_1), \cdots, L^{l-2}(F_\gamma) = (-Q_{l-2}, 2P_{l-2}, Q_{l-3}), \\ & L^{l-1}(F_\gamma) = (Q_{l-1}, 2P_{l-1}, -Q_{l-2}), L^l(F_\gamma) = (-Q_0, 2P_0, Q_0), \\ & L^{l+1}(F_\gamma) = (Q_1, 2P_1, -Q_0), \cdots, L^{2l-1}(F_\gamma) = (-Q_{l-1}, 2P_{l-1}, Q_{l-2}), \\ & L^{2l}(F_\gamma) = (Q_0, 2P_0, -Q_0) = F_\gamma \end{aligned}$$

as we wanted.

(2) Let $Q = 1$. Then $R^1(F_\gamma) = (-1, 2P, 1), R^2(F_\gamma) = (1, 2P, -1) = F_\gamma, L^1(F_\gamma) = (-1, 2P, 1), L^2(F_\gamma) = (1, 2P, -1) = F_\gamma$. So F_γ has one right and one left neighbor and they are same, namely, $R^1(F_\gamma) = L^1(F_\gamma) = (-1, 2P, 1)$. □

Example 2.3. Let $p = 13$. Then the cycle of $I_\gamma = [3, 2 + \sqrt{13}]$ is $I_{\gamma_0} = [3, 2 + \sqrt{13}] \sim I_{\gamma_1} = [4, 1 + \sqrt{13}] \sim I_{\gamma_2} = [1, 3 + \sqrt{13}] \sim I_{\gamma_3} = [4, 3 + \sqrt{13}] \sim I_{\gamma_4} = [3, 1 + \sqrt{13}]$ of length 5. So the right neighbors of $F_\gamma = (3, 4, -3)$ are

$$\begin{aligned} & R^1(F_\gamma) = (-3, 2, 4), R^2(F_\gamma) = (4, 6, -1), R^3(F_\gamma) = (-1, 6, 4), \\ & R^4(F_\gamma) = (4, 2, -3), R^5(F_\gamma) = (-3, 4, 3), R^6(F_\gamma) = (3, 2, -4), \\ & R^7(F_\gamma) = (-4, 6, 1), R^8(F_\gamma) = (1, 6, -4), R^9(F_\gamma) = (-4, 2, 3) \end{aligned}$$

and the left neighbors of F_γ are

$$L^1(F_\gamma)=(-4,2,3), L^2(F_\gamma)=(1,6,-4), L^3(F_\gamma)=(-4,6,1),$$
$$L^4(F_\gamma)=(3,2,-4), L^5(F_\gamma)=(-3,4,3), L^6(F_\gamma)=(4,2,-3),$$
$$L^7(F_\gamma)=(-1,6,4), L^8(F_\gamma)=(4,6,-1), L^9(F_\gamma)=(-3,2,4).$$

Here, we note that $R^5(F_\gamma)=L^5(F_\gamma)=(-3,4,3)$.

From Theorem 2.2, we can give the following result.

COROLLARY 2.4. *If $Q\neq 1$, then we have*

(1) $R^i(F_\gamma)=\tau(R^{i-l}(F_\gamma))$ *and* $L^i(F_\gamma)=\tau(L^{i-l}(F_\gamma))$ *for* $l\leq i\leq 2l-1$.

(2) $R^i(F_\gamma)=L^{2l-i}(F_\gamma)$ *for* $1\leq i\leq 2l-1$ *and so the* l^{th} *right and left neighbors of* F_γ *are the same, that is,* $R^l(F_\gamma)=L^l(F_\gamma)=(-Q_0,2P_0,Q_0)$.

For the second part of this work, we can give the following results.

THEOREM 2.5. *Let γ be the quadratic irrational in* (2.2).

(1) *If $Q\neq 1$, then the continued fraction expansion of γ is*

$$[\overline{m_0,m_1,m_2,\cdots,m_{\frac{l-3}{2}},m_{\frac{l-1}{2}},m_{\frac{l-3}{2}},\cdots,m_2,m_1,m_0}]$$

of length l and the continued fraction expansion of $\sqrt{p}$ is

$$\left[\frac{m_{\frac{l-1}{2}}}{2};\overline{m_{\frac{l-3}{2}},m_{\frac{l-5}{2}},\cdots,m_1,m_0,m_0,m_1,\cdots,m_{\frac{l-3}{2}},m_{\frac{l-1}{2}}}\right]$$

of length l.

(2) *If $Q=1$, then the continued fraction expansion of γ is $[\overline{2P}]$ of length 1 and the continued fraction expansion of $\sqrt{p}$ is $[P;\overline{2P}]$ of length 1.*

Proof. (1) Let $Q\neq 1$. Then from Table 1, we easily seen that the continued fraction expansion of γ is $[\overline{m_0,m_1,\cdots,m_{\frac{l-3}{2}},m_{\frac{l-1}{2}},m_{\frac{l-3}{2}},\cdots,m_1,m_0}]$. Notice that $\lfloor\sqrt{p}\rfloor=\frac{m_{\frac{l-1}{2}}}{2}$. So we get

$$\sqrt{p}=\frac{m_{\frac{l-1}{2}}}{2}+\left(\sqrt{p}-\frac{m_{\frac{l-1}{2}}}{2}\right)=\frac{m_{\frac{l-1}{2}}}{2}+\cfrac{1}{\cfrac{\sqrt{p}+\frac{m_{\frac{l-1}{2}}}{2}}{p-\left(\frac{m_{\frac{l-1}{2}}}{2}\right)^2}}$$

$$=\frac{m_{\frac{l-1}{2}}}{2}+\cfrac{1}{m_{\frac{l-3}{2}}+\cfrac{\sqrt{p}+\frac{m_{\frac{l-1}{2}}}{2}-m_{\frac{l-3}{2}}\left[p-\left(\frac{m_{\frac{l-1}{2}}}{2}\right)^2\right]}{p-\left(\frac{m_{\frac{l-1}{2}}}{2}\right)^2}}$$

$$=\cdots$$

$$= \frac{m_{\frac{l-1}{2}}}{2} + \cfrac{1}{m_{\frac{l-3}{2}} + \cfrac{\sqrt{p}+\frac{m_{\frac{l-1}{2}}}{2} - m_{\frac{l-3}{2}}\left[p-\left(\frac{m_{\frac{l-1}{2}}}{2}\right)^2\right]}{p-\left(\frac{m_{\frac{l-1}{2}}}{2}\right)^2}}$$

$$= \frac{m_{\frac{l-1}{2}}}{2} + \cfrac{1}{m_{\frac{l-3}{2}} + \cfrac{1}{m_{\frac{l-5}{2}} + \cfrac{1}{\ddots + m_{\frac{l-1}{2}} + \left(\sqrt{p} - \frac{m_{\frac{l-1}{2}}}{2}\right)}}}.$$

Hence $\sqrt{p}=\left[\frac{m_{\frac{l-1}{2}}}{2};\overline{m_{\frac{l-3}{2}},m_{\frac{l-5}{2}},\cdots,m_1,m_0,m_0,m_1,\cdots,m_{\frac{l-3}{2}},m_{\frac{l-1}{2}}}\right]$ of length l.

(2) Let $Q = 1$. Then $m_0 = 2P$, $P_1 = P = P_0$ and $Q_1 = 1 = Q_0$, we get $\gamma = [\overline{2P}]$. Also since $p = P^2 + 1$, we get

$$\sqrt{p} = P + (\sqrt{p} - P) = P + \frac{1}{\frac{\sqrt{p}+P}{p-P^2}} = P + \frac{1}{2P + (\sqrt{p} - P)},$$

that is, $\sqrt{p} = \left[P; \overline{2P}\right]$ of length 1 as we claimed. $\square$

Remark 2.6. We note in (2.1) that, we take $P = b$ and $Q = |a|$. If we take $P = |a|$ and $Q = b$, then we cannot deduce the continued fraction expansion of $\sqrt{p}$ from the continued fraction expansion of γ. Indeed, for $p = 73$, we have

$$\gamma = \begin{cases} [\overline{5, 1, 1, 16, 1, 1, 5}] & \text{if } P = 8, Q = 3 \\ [\overline{1, 2, 3, 1, 7, 1, 3, 2, 1}] & \text{if } P = 3, Q = 8. \end{cases}$$

Note that $\sqrt{73} = [8; \overline{1, 1, 5, 5, 1, 1, 16}]$. Similarly for $p = 137$, we have

$$\gamma = \begin{cases} [\overline{1, 2, 2, 1, 22, 1, 2, 2, 1}] & \text{if } P = 4, Q = 11 \\ [\overline{5, 1, 2, 11, 2, 1, 5}] & \text{if } P = 11, Q = 4. \end{cases}$$

But $\sqrt{137} = [11; \overline{1, 2, 2, 1, 1, 2, 2, 1, 22}]$. So that is why we take $P = b$ and $Q = |a|$.

We can deduce the set of proper automorphisms of F_γ in (2.4) by using the continued fraction expansion of γ. For the matrix defined in (1.2), we set

$$T(\delta) = \begin{bmatrix} 0 & -1 \\ 1 & -\delta \end{bmatrix}^{-1} = \begin{bmatrix} -\delta & 1 \\ -1 & 0 \end{bmatrix}$$

and define $g_{F,n} = T(\delta_0)T(\delta_1)\cdots T(\delta_{n-1})$, where δ is defined in (1.3). Then we can give the following theorem.

THEOREM 2.7. *Let the continued fraction expansion of γ be as in Theorem 2.5.*

(1) If $Q \neq 1$, then the set of proper automorphisms of F_γ is

$$Aut^+(F_\gamma) = \{\pm(g_{F_\gamma,2l})^t : t \in \mathbb{Z}\},$$

where

$$g_{F_\gamma,2l} = \prod_{i=0}^{2l-1} T(\delta_i) \ \ and \ \ \delta_i = \begin{cases} (-1)^{i+1}m_i & for\ 0 \leq i \leq l-1 \\ (-1)^{i-l}m_{i-l} & for\ l \leq i \leq 2l-1. \end{cases}$$

(2) If $Q = 1$, then the set of proper automorphisms of F_γ is

$$Aut^+(F_\gamma) = \{\pm(g_{F_\gamma,2})^t : t \in \mathbb{Z}\},$$

where

$$g_{F_\gamma,2} = \begin{bmatrix} -4P^2-1 & 2P \\ 2P & -1 \end{bmatrix}.$$

Proof. (1) Let $Q \neq 1$. We proved in Theorem 2.2 that $R^i(F_\gamma) = ((-1)^{i+2}Q_{i-1}, 2P_i, (-1)^{i+1}Q_i), R^{l+i}(F_\gamma) = ((-1)^{i+1}Q_{i-1}, 2P_i, (-1)^{i+2}Q_i)$ for $1 \leq i \leq l-1$ and $R^l(F_\gamma) = (-Q_0, 2P_0, Q_0)$, $\delta_i = (-1)^{i+1}s_i$ for $0 \leq i \leq l-1$ and $\delta_i = (-1)^{i-l}s_{i-l}$ for $l \leq i \leq 2l-1$. For the form $F_i = (Q_i, 2P_i, -Q_i)$ of discriminant $\Delta = 4p$, we have

$$s_i = \left\lfloor \frac{b_i + \sqrt{\Delta}}{2|c_i|} \right\rfloor = \left\lfloor \frac{2P_i + \sqrt{4p}}{2|-Q_i|} \right\rfloor = \left\lfloor \frac{P_i + \sqrt{p}}{Q_i} \right\rfloor = m_i.$$

So $\delta_i = (-1)^{i+1}m_i$ for $0 \leq i \leq l-1$ and $\delta_i = (-1)^{i-l}m_{i-l}$ for $l \leq i \leq 2l-1$. Thus $g_{F,2l} = T(\delta_0)T(\delta_1)\cdots T(\delta_{2l-1})$ by [4, Theorem 9.4] since $R^{2l}(F_\gamma) = F_\gamma$. Therefore, the set of proper automorphisms of F_γ is $Aut^+(F_\gamma) = \{\pm(g_{F_\gamma,2l})^t : t \in \mathbb{Z}\}$.

(2) Let $Q = 1$. Since $R^2(F_\gamma) = F_\gamma$ for $F_\gamma = (1, 2P, -1)$, we get

$$g_{F,2} = T(\delta_0)T(\delta_1) = \begin{bmatrix} -4P^2-1 & 2P \\ 2P & -1 \end{bmatrix}$$

and hence $Aut^+(F_\gamma) = \{\pm(g_{F_\gamma,2})^t : t \in \mathbb{Z}\}$. □

Example 2.8. **1)** Let $p = 13$. Then $\gamma = \frac{2+\sqrt{13}}{3} = [\overline{1,1,6,1,1}]$. So

$$g_{F_\gamma,10} = \prod_{i=0}^{9} T(\delta_i) = \begin{bmatrix} -1009 & 540 \\ 540 & -289 \end{bmatrix}.$$

Hence $Aut^+(F_\gamma) = \{\pm(g_{F_\gamma,10})^t : t \in \mathbb{Z}\}$ for $F_\gamma = (3, 4, -3)$.

2) Let $p = 73$. Then $\gamma = \frac{8+\sqrt{73}}{3} = [\overline{5, 1, 1, 16, 1, 1, 5}]$. So

$$g_{F_\gamma,14} = \prod_{i=0}^{13} T(\delta_i) = \begin{bmatrix} -4417249 & 801000 \\ 801000 & -145249 \end{bmatrix}.$$

Hence $Aut^+(F_\gamma) = \{\pm(g_{F_\gamma,14})^t : t \in \mathbb{Z}\}$ for $F_\gamma = (3, 16, -3)$.

3) Let $p = 17$. Then $\gamma = 4 + \sqrt{17} = [\overline{8}]$. So

$$g_{F,2} = T(\delta_0)T(\delta_1) = \begin{bmatrix} -65 & 8 \\ 8 & -1 \end{bmatrix}.$$

Hence $Aut^+(F_\gamma) = \{\pm(g_{F_\gamma,2})^t : t \in \mathbb{Z}\}$ for $F_\gamma = (1, 8, -1)$.

From Theorems 2.1 and 2.5, we can give the following result.

Corollary 2.9. *If $Q \neq 1$, then in the cycle of I_γ, we have $Q_i = Q_{l-1-i}$ for $0 \leq i \leq l-1$ and $P_i = P_{l-i}$ for $1 \leq i \leq l-1$, and in the continued faction expansion of γ, we have $m_i = m_{l-1-i}$ for $0 \leq i \leq l-1$.*

Now we can consider the Pell equations. Recall that the fundamental solution of the Pell equation

$$x^2 - py^2 = \pm 1$$

is very important to find all other integer solutions. In the following theorem, we prove that the fundamental solution of the Pell equation can be obtained from the continued fraction expansion of γ.

Theorem 2.10. *Let the continued fraction expansion of γ be as in Theorem 2.5.*

(1) *If $Q \neq 1$, then the fundamental solution of $x^2 - py^2 = 1$ is (A_{2l-1}, B_{2l-1}), where*

$$A_{2l-1} + B_{2l-1}\sqrt{p} = \prod_{i=0}^{2l-1} \gamma_i$$

and the fundamental solution of $x^2 - py^2 = -1$ is (A_{l-1}, B_{l-1}), where

$$A_{l-1} + B_{l-1}\sqrt{p} = \prod_{i=0}^{l-1} \gamma_i.$$

(2) *If $Q = 1$, then the fundamental solution of $x^2 - py^2 = 1$ is $(x_1, y_1) = (2P^2+1, 2P)$ and the fundamental solution of $x^2 - py^2 = -1$ is $(x_1, y_1) = (P, 1)$.*

Proof. First we note that $N(\gamma_i) = \frac{P_i^2 - p}{Q_i^2} = \frac{-Q_i^2}{Q_i^2} = -1$ for $\gamma_i = \frac{P_i + \sqrt{p}}{Q_i}$. Therefore

$$N(\prod_{i=0}^{2l-1} \gamma_i) = N(\gamma_0)N(\gamma_1)\cdots N(\gamma_{2l-1}) = (-1)^{2l} = 1.$$

(1) Let $Q \neq 1$. Then from Theorem 2.5, the continued fraction expansion of $\sqrt{p}$ is

$$\left[\frac{m_{\frac{l-1}{2}}}{2}; \overline{m_{\frac{l-3}{2}}, \cdots, m_1, m_0, m_0, m_1, \cdots, m_{\frac{l-3}{2}}, m_{\frac{l-1}{2}}}\right].$$

Since l is odd, the fundamental solution of $x^2 - py^2 = 1$ is $(x_1, y_1) = (A_{2l-1}, B_{2l-1})$ by Lemma 1.3. On the other hand, it can be easily seen that $\prod_{i=0}^{2l-1} \gamma_i = A_{2l-1} + B_{2l-1}\sqrt{p}$. Similarly, it can be shown that $\prod_{i=0}^{l-1} \gamma_i = A_{l-1} + B_{l-1}\sqrt{p}$.

(2) Let $Q = 1$. Since $\sqrt{p} = [P; \overline{2P}]$, we get $A_0 = P, A_1 = 2P^2 + 1, B_0 = 1$ and $B_1 = 2P$. So the result is obvious. □

Example 2.11. **1)** Let $p = 53$. Since $\sqrt{53} = [7; \overline{3, 1, 1, 3, 14}]$, we get $A_4 = 182$, $A_9 = 66249, B_4 = 25$ and $B_9 = 9100$. So the fundamental solution of $x^2 - 53y^2 = 1$ is $(x_1, y_1) = (66249, 9100)$ and the fundamental solution of $x^2 - 53y^2 = -1$ is $(x_1,\, y_1) = (182, 25)$. Note that

$$\prod_{i=0}^{9} \gamma_i = 66249 + 9100\sqrt{53} \quad \text{and} \quad \prod_{i=0}^{4} \gamma_i = 182 + 25\sqrt{53}$$

for $\gamma = \frac{2+\sqrt{53}}{7} = [\overline{1, 3, 14, 3, 1}]$.

2) Let $p = 113$. Since $\sqrt{113} = [10; \overline{1, 1, 1, 2, 2, 1, 1, 1, 20}]$, we get $A_8 = 776, A_{17} = 1204353, B_8 = 73, B_{17} = 113296$. So the fundamental solution of $x^2 - 113y^2 = 1$ is $(x_1, y_1) = (1204353, 113296)$ and the fundamental solution of $x^2 - 113y^2 = -1$ is $(x_1, y_1) = (776, 73)$. Note that

$$\prod_{i=0}^{17} \gamma_i = 1204353 + 113296\sqrt{113} \quad \text{and} \quad \prod_{i=0}^{8} \gamma_i = 776 + 73\sqrt{113}$$

for $\gamma = \frac{8+\sqrt{113}}{7} = [\overline{2, 1, 1, 1, 20, 1, 1, 1, 2}]$.

3) Let $p = 101$. Then $\sqrt{101} = [10; \overline{20}]$ and hence $A_0 = 10, A_1 = 201, B_0 = 1$, $B_1 = 20$. Therefore the fundamental solution of $x^2 - 101y^2 = 1$ is $(x_1, y_1) = (201, 20)$ and the fundamental solution of $x^2 - 101y^2 = -1$ is $(x_1, y_1) = (10, 1)$. Also $\prod_{i=0}^{1} \gamma_i = 201 + 20\sqrt{101}$ and $\prod_{i=0}^{0} \gamma_i = 10 + \sqrt{101}$ for $\gamma = 10 + \sqrt{101} = [\overline{20}]$.

For an integral quadratic form F, we set

$$Aut^{*}(F)=\{g\in \mathrm{GL}(2,\mathbb{Z}):gF=-F \text{ with } \det(g)=-1\}.$$

From above theorem, we can give the following result.

THEOREM 2.12. *Let F_γ be the form defined in (2.4) and let A_{l-1}, B_{l-1} be as in Theorem 2.10.*

(1) *If $Q\neq 1$, then $Aut^{*}(F_\gamma)=\{\pm(g_\gamma^{*})^{2t+1}:t\in\mathbb{Z}\}$, where*

$$g_\gamma^{*}=\begin{bmatrix} A_{l-1}-PB_{l-1} & QB_{l-1}\\ QB_{l-1} & A_{l-1}+PB_{l-1}\end{bmatrix}.$$

(2) *If $Q=1$, then $Aut^{*}(F_\gamma)=\{\pm(g_\gamma^{1*})^{2t+1}:t\in\mathbb{Z}\}$, where*

$$g_\gamma^{1*}=\begin{bmatrix} 0 & 1\\ 1 & 2P\end{bmatrix}.$$

Proof. (1) Let $Q\neq 1$. First we note that

$$\begin{aligned}\det(g_\gamma^{*})&=(A_{l-1}-PB_{l-1})(A_{l-1}+PB_{l-1})-(QB_{l-1})^2\\&=A_{l-1}^2-(P^2+Q^2)B_{l-1}^2\\&=A_{l-1}^2-pB_{l-1}^2\\&=-1\end{aligned}$$

since (A_{l-1},B_{l-1}) is the fundamental solution of the Pell equation $x^2-py^2=-1$. From (1.1), we get

$$\begin{aligned}g_\gamma^{*}F_\gamma&=F_\gamma((A_{l-1}-PB_{l-1})x+QB_{l-1}y,QB_{l-1}x+(A_{l-1}+PB_{l-1})y)\\&=Q((A_{l-1}-PB_{l-1})x+QB_{l-1}y)^2+2P((A_{l-1}-PB_{l-1})x+QB_{l-1}y)\\&\quad\times(QB_{l-1}x+(A_{l-1}+PB_{l-1})y)-Q(QB_{l-1}x+(A_{l-1}+PB_{l-1})y)^2\\&=x^2\left\{Q(A_{l-1}-PB_{l-1})^2+2PQB_{l-1}(A_{l-1}-PB_{l-1})-Q^3B_{l-1}^3\right\}\\&\quad+xy\left\{\begin{array}{c}2Q^2B_{l-1}(A_{l-1}-PB_{l-1})+2P(A_{l-1}-PB_{l-1})\times\\(A_{l-1}+PB_{l-1})+2PQ^2B_{l-1}^2-2Q^2B_{l-1}(A_{l-1}+PB_{l-1})\end{array}\right\}\\&\quad+y^2\left\{Q^3B_{l-1}^2+2PQB_{l-1}(A_{l-1}+PB_{l-1})-Q(A_{l-1}+PB_{l-1})^2\right\}\\&=(A_{l-1}^2-pB_{l-1}^2)(Qx^2+2Pxy-Qy^2)\\&=-Qx^2-2Pxy+Qy^2\\&=-F_\gamma(x,y).\end{aligned}$$

So $g_\gamma^{*}\in Aut^{*}(F_\gamma)$. It can be proved by induction on t that $\pm(g_\gamma^{*})^{2t+1}\in Aut^{*}(F_\gamma)$ for $t\in\mathbb{Z}$. So $Aut^{*}(F_\gamma)=\{\pm(g_\gamma^{*})^{2t+1}:t\in\mathbb{Z}\}$.

Statement (2) can be proved similarly. □

Remark 2.13. **(1)** In the above theorem, we note that odd powers of g_γ^* are the elements of $Aut^*(F_\gamma)$, that is, $Aut^*(F_\gamma) = \{\pm(g_\gamma^*)^{2t+1} : t \in \mathbb{Z}\}$. In fact, even powers of g_γ^* are the proper automorphisms of F_γ.

(2) There is a connection between $g_{F_\gamma,2l}$ and g_γ^* and also $g_{F_\gamma,2}$ and g_γ^{1*} obtained in Theorems 2.7 and 2.12 which is given below.

THEOREM 2.14. *For the matrices $g_{F_\gamma,2l}, g_\gamma^*$ and $g_{F_\gamma,2}, g_\gamma^{1*}$, we have*

$$-(g_\gamma^*)^{-2} = g_{F_\gamma,2l} \quad \textit{and} \quad -(g_\gamma^{1*})^{-2} = g_{F_\gamma,2}.$$

Proof. For g_γ^*, we easily have

$$-(g_\gamma^*)^{-2} = \begin{bmatrix} -A_{l-1}^2 - pB_{l-1}^2 - 2PA_{l-1}B_{l-1} & 2QA_{l-1}B_{l-1} \\ 2QA_{l-1}B_{l-1} & -A_{l-1}^2 - pB_{l-1}^2 + 2PA_{l-1}B_{l-1} \end{bmatrix}.$$

On the other hand, it can be proved by induction on l that

$$g_{F_\gamma,2l} = \begin{bmatrix} -A_{l-1}^2 - pB_{l-1}^2 - 2PA_{l-1}B_{l-1} & 2QA_{l-1}B_{l-1} \\ 2QA_{l-1}B_{l-1} & -A_{l-1}^2 - pB_{l-1}^2 + 2PA_{l-1}B_{l-1} \end{bmatrix}.$$

So $-(g_\gamma^*)^{-2} = g_{F_\gamma,2l}$. Similarly for g_γ^{1*}, we have

$$-(g_\gamma^{1*})^{-2} = \begin{bmatrix} -4P^2 - 1 & 2P \\ 2P & -1 \end{bmatrix} = g_{F_\gamma,2}$$

as we wanted. □

Example 2.15. Let $p = 13$. Then

$$g_{F_\gamma,10} = \begin{bmatrix} -1009 & 540 \\ 540 & -289 \end{bmatrix} \text{ and } g_\gamma^* = \begin{bmatrix} 8 & 15 \\ 15 & 28 \end{bmatrix}.$$

Here $-(g_\gamma^*)^{-2} = g_{F_\gamma,10}$. Let $p = 73$. Then

$$g_{F_\gamma,14} = \begin{bmatrix} -4417249 & 801000 \\ 801000 & -145249 \end{bmatrix} \text{ and } g_\gamma^* = \begin{bmatrix} 68 & 375 \\ 375 & 2068 \end{bmatrix}.$$

Again $-(g_\gamma^*)^{-2} = g_{F_\gamma,14}$.

Finally, we can consider the equation

$$x^2 - py^2 = \pm p.$$

Before considering all integer solutions we need some notations: Let Δ be a non–square discriminant. Then the $\Delta-$order O_Δ is defined for non–square discriminants Δ to be the ring $O_\Delta = \{x + y\rho_\Delta : x, y \in \mathbb{Z}\}$, where $\rho_\Delta = \sqrt{\frac{\Delta}{4}}$ if $\Delta \equiv 0(\text{mod } 4)$ or $\rho_\Delta = \frac{1+\sqrt{\Delta}}{2}$ if $\Delta \equiv 1(\text{mod } 4)$. So O_Δ is a subring of $\mathbb{Q}(\sqrt{\Delta})$ $=\{x + y\sqrt{\Delta} : x, y \in \mathbb{Q}\}$. The unit group O_Δ^* is defined for non–square discriminants Δ to be the group of units of the ring O_Δ.

The module M_F of an integral form F is $M_F = \{xa + y\frac{b+\sqrt{\Delta}}{2} : x, y \in \mathbb{Z}\} \subset \mathbb{Q}(\sqrt{\Delta})$. So we get $(u + v\rho_\Delta)(xa + y\frac{b+\sqrt{\Delta}}{2}) = x'a + y'\frac{b+\sqrt{\Delta}}{2}$, where

$$(2.5) \qquad [x' \quad y'] = \begin{cases} [x \quad y]\begin{bmatrix} u - \frac{b}{2}v & av \\ -cv & u + \frac{b}{2}v \end{bmatrix} & \text{if } \Delta \equiv 0(\text{mod } 4) \\ [x \quad y]\begin{bmatrix} u + \frac{1-b}{2}v & av \\ -cv & u + \frac{1+b}{2}v \end{bmatrix} & \text{if } \Delta \equiv 1(\text{mod } 4). \end{cases}$$

Therefore, there is a bijection

$$\Psi : \Omega = \{(x, y) : F(x, y) = m\} \to \{\gamma \in M_F : N(\gamma) = am\}$$

for solving the equation $F(x, y) = m$. The action of $O^*_{\Delta,1} = \{\alpha \in O^*_\Delta : N(\alpha) = 1\}$ on the set Ω is the most interesting when Δ is a positive non–square since $O^*_{\Delta,1}$ is infinite. So the orbit of each solution will then be infinite and hence the set Ω is either empty or infinite. Since $O^*_{\Delta,1}$ can be explicitly determined, Ω is satisfactorily described by the representation of such a list, called a **set of representatives** of the orbits. Let ε_Δ be the **smallest unit** of O_Δ that is greater than 1 and let $\tau_\Delta = \varepsilon_\Delta$ if $N(\varepsilon_\Delta) = 1$; or ε^2_Δ if $N(\varepsilon_\Delta) = -1$. Then every $O^*_{\Delta,1}$ orbit of integral solutions of $F(x, y) = m$ contains a solution $(x, y) \in \mathbb{Z}^2$ such that $0 \leq y \leq U$, where $U = \left|\frac{am\tau_\Delta}{\Delta}\right|^{\frac{1}{2}}(1 - \frac{1}{\tau_\Delta})$ if $am > 0$ or $U = \left|\frac{am\tau_\Delta}{\Delta}\right|^{\frac{1}{2}}(1 + \frac{1}{\tau_\Delta})$ if $am < 0$. So for finding a set of representatives of the $O^*_{\Delta,1}$ orbits of $F(x, y) = m$, we must determine for which values of y, $\Delta y^2 + 4am$ is a perfect square in the range $0 \leq y \leq U$ since $\Delta y^2 + 4am = (2ax + by)^2$.

We note that we can determine A_{2l-1} and B_{2l-1} in Theorem 2.10 from the continued fraction expansion of γ. Thus we can give the following theorem.

THEOREM 2.16. *For the Pell equation $x^2 - py^2 = \pm p$, we have*

(1) *If $Q \neq 1$, then the set of all positive integer solutions of $x^2 - py^2 = p$ is $\Omega = \{(x_n, y_n)\}$, where*

$$[x_n \quad y_n] = [\sqrt{p(U^2 + 1)} \quad -U]M^n$$

for $n \geq 1$, and the set of all positive integer solutions of $x^2 - py^2 = -p$ is $\Omega = \{(x_n, y_n)\}$, where

$$[x_n \quad y_n] = [0 \quad 1]M^n$$

for $n \geq 1$ with $M = \begin{bmatrix} A_{2l-1} & B_{2l-1} \\ pB_{2l-1} & A_{2l-1} \end{bmatrix}$.

(2) *If $Q = 1$, then the set of all positive integer solutions of $x^2 - py^2 = p$ is $\Omega = \{(x_n, y_n)\}$, where*

$$[x_n \quad y_n] = [p \quad -P]M^n$$

for $n \geq 1$, and the set of all positive integer solutions of $x^2 - py^2 = -p$

is $\Omega = \{(x_n, y_n)\}$, *where*

$$[x_n \quad y_n] = [0 \quad 1]M^n$$

for $n \geq 1$ *with* $M = \begin{bmatrix} 2P^2+1 & 2P \\ 2P^3+2P & 2P^2+1 \end{bmatrix}$.

Proof. (1) Let $Q \neq 1$. Then we proved in Theorem 2.10 that the fundamental solution $x^2 - py^2 = \pm 1$ can be obtained from the continued fraction expansion of γ, that is, we can determine the integers A_{2l-1} and B_{2l-1} depending on γ. For the equation $x^2 - py^2 = p$, we have $\tau_\Delta = A_{2l-1} + B_{2l-1}\sqrt{p}$ and $\Delta y^2 + 4am = 4p(y^2+1)$ is a square only for $y = U$ in the range $0 \leq y \leq U$, where $U = \frac{1}{2}\frac{A_{2l-1}-1+B_{2l-1}\sqrt{p}}{\sqrt{A_{2l-1}+B_{2l-1}\sqrt{p}}}$. So $x = \pm\sqrt{p(U^2+1)}$ and hence $\{[\pm\sqrt{p(U^2+1)} \quad U]\}$ is a set of representatives and thus $[\sqrt{p(U^2+1)} \quad -U]M^n$ generates the solutions (x_n, y_n) for $n \geq 1$, where M is defined as above. So the set of all positive integer solutions of $x^2 - py^2 = p$ is $\Omega = \{(x_n, y_n)\}$, where $[x_n \quad y_n] = [\sqrt{p(U^2+1)} \quad -U]M^n$ for $n \geq 1$. For the equation $x^2 - py^2 = -p$, we see that $\{[0 \quad 1]\}$ is a set of representatives and $[0 \quad 1]M^n$ generates the solutions (x_n, y_n) for $n \geq 1$. Thus the set of all positive integer solutions of $x^2 - py^2 = -p$ is $\Omega = \{(x_n, y_n)\}$, where $[x_n \quad y_n] = [0 \quad 1]M^n$ for $n \geq 1$.

(2) Let $Q = 1$. Then for the equation $x^2 - py^2 = p$, we have $\tau_\Delta = 2P^2 + 1 + 2P\sqrt{p}$ and in the range $0 \leq y \leq P$, $\Delta y^2 + 4am$ is a square only for $y = P$. Hence we get $x = \pm p$. So $\{[\pm p \quad P]\}$ is a set of representatives and $[p \quad -P]M^n$ generates the solutions (x_n, y_n) for $n \geq 1$, where M is defined as above. For the equation $x^2 - py^2 = -p$, we see that $\{[0 \quad 1]\}$ is a set of representatives and $[0 \quad 1]M^n$ generates the solutions (x_n, y_n) for $n \geq 1$. This completes the proof. ☐

Example 2.17. **1)** Let $p = 73$. Then $A_{13} = 2281249$, $B_{13} = 267000$ and hence $U = 1068$. In the range $0 \leq y \leq 1068$, $292(y^2+1)$ is square only for $y = 1068$ and hence $x = \pm 9125$. So $\{[\pm 9125 \quad 1068]\}$ is a set of representatives. Therefore, the set of all positive integer solutions of $x^2 - 73y^2 = 73$ is $\Omega = \{(x_n, y_n)\}$, where

$$[x_n \quad y_n] = [9125 \quad -1068]\begin{bmatrix} 2281249 & 267000 \\ 19491000 & 2281249 \end{bmatrix}^n$$

for $n \geq 1$. For the equation $x^2 - 73y^2 = -73$, $292(y^2-1)$ is square only for $y = 1$ in the range $0 \leq y \leq 1068$ and hence $x = 0$. So $\{[0 \quad 1]\}$ is a set of representatives. So the set of all positive integer solutions of $x^2 - 73y^2 = -73$ is $\Omega = \{(x_n, y_n)\}$, where

$$[x_n \quad y_n] = [0 \quad 1]\begin{bmatrix} 2281249 & 267000 \\ 19491000 & 2281249 \end{bmatrix}^n$$

for $n \geq 1$.

2) Let $p = 37$. Then in the range $0 \leq y \leq 6$, $148(y^2+1)$ is square only for $y = 6$ and hence $x = \pm 37$. So $\{[\pm 37 \;\; 6]\}$ is a set of representatives. Therefore, the set of all positive integer solutions of $x^2 - 37y^2 = 37$ is $\Omega = \{(x_n, y_n)\}$, where

$$[x_n \;\; y_n] = [37 \;\; -6] \begin{bmatrix} 73 & 12 \\ 444 & 73 \end{bmatrix}^n$$

for $n \geq 1$. For the equation $x^2 - 37y^2 = -37$, $148(y^2 - 1)$ is square only for $y = 1$ in the range $0 \leq y \leq 6$ and hence $x = 0$. So $\{[0 \;\; 1]\}$ is a set of representatives. Thus $\Omega = \{(x_n, y_n)\}$, where

$$[x_n \;\; y_n] = [0 \;\; 1] \begin{bmatrix} 73 & 12 \\ 444 & 73 \end{bmatrix}^n$$

for $n \geq 1$.

REFERENCES

[1] E. Barbeau, *Pell's Equation.* Springer-Verlag, 2003.

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

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

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

[5] M. Jacobson and H. Williams, *Solving the Pell Equation, CMS Books in Mathematics.* Springer, 2010.

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

[7] R.A. Mollin, *Fundamental Number Theory with Applications. Second Edition.* Discrete Math. Appl., Chapman & Hall/ CRC, Boca Raton, London, New York, 2008.

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

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

[10] A. Tekcan, *Proper Cycles of Indefinite Quadratic Forms and their Right Neighbors.* Appl. Math. **52**(5) (2007), 407–415.

[11] A. Tekcan, A. Özkoç and İ.N. Cangül, *Indefinite Quadratic Forms and their Neighbours.* Numerical Anal. Appl. Math. ICNAAM 2011 AIP Conf. Proc. **1281** (2010), 1102–1105.

Received 5 November 2015

Uludag University,
Faculty of Science,
Department of Mathematics,
Bursa–Turkiye
tekcan@uludag.edu.tr