Turk J Math
24 (2000) , 209 – 220.

Conjugacy Classes of Elliptic Elements in the Picard Group

Nihal Yılmaz, İ. Naci Cangül

Abstract

The Picard group **P** is a discrete subgroup of $PSL(2,\mathbb{C})$ with Gaussian integer coefficients. Here it is shown that the total number of conjugacy classes of elliptic elements of order 2 and 3 in **P**, which is given as seven by B. Fine [3], can actually be reduced to four and using this, the conditions for the maximal Fuchsian subgroups of **P** to have elliptic elements of orders 2 and 3 are found.

1. Introduction

The extension $\mathbb{Z}(i) = \left\{m + in : m, n \in \mathbb{Z}, i^2 = -1\right\}$ of $\mathbb{Z}$ forms a ring called the ring of Gaussian integers. Each element of $\mathbb{Z}(i)$ is called a Gaussian integer.

The Picard group is denoted by **P** and contains all linear fractional transformations

$$t(z) = \frac{az + b}{cz + d}$$

where $a, b, c, d \in \mathbb{Z}(i)$ and $ad - bc = 1$. Therefore $\mathbf{P} = PSL(2, \mathbb{Z}(i))$. **P** is an important subgroup of $PSL(2,\mathbb{C})$. It is an example to that the discreteness on $\widehat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ does not imply the discontinuity. Although its action on $\widehat{\mathbb{C}}$ is not discontinuous, its action on the hyperbolic 3-space

$$\mathbb{H}^3 = \{z + tj : z \in \mathbb{C}, t > 0\}$$

is discontinuous, [1]. Actually **P** has a well-known presentation

$$\mathbf{P} = \left\langle x, u, y, r; x^3 = u^2 = y^3 = r^2 = (xu)^2 = (xy)^2 = (ry)^2 = (ru)^2 = 1 \right\rangle \tag{1.1}$$

where

$$x(z) = \frac{i}{iz+1}, u(z) = -\frac{1}{z}, y(z) = \frac{z+1}{-z}, r(z) = \frac{i}{iz}. \tag{1.2}$$

This presentation is obtained by looking at the orders of rotations which act around the vertices of a fundamental polyhedron for **P** in $\mathbb{H}^3$ and then by finding the relations between the edges of this polyhedron (called side pairings), [2].

P is given abstractly as an amalgamated free product of two groups G_1, G_2 with the modular group **M** as the amalgamated subgroup. Namely $\mathbf{P} \cong G_1 *_{\mathbf{M}} G_2$ with $G_1 \cong S_3 *_{\mathbb{Z}_3} A_4$ and $G_2 \cong S_3 *_{\mathbb{Z}_2} D_2$ (S_3 is the symmetric group on three symbols, A_4 is the alternating group on four symbols and D_2 is the Klein 4-group), [4].

2. Conjugacy classes in P and maximal Fuchsian subgroups

Let $t \in \mathbf{P}$ be elliptic. It is known that such a t is conjugate to the transformation $z \to \lambda z$ with $|\lambda| = 1$ in $PSL(2, \mathbb{C})$, [7]. But we need to know the conjugacy classes in **P** of elliptic elements when studying Fuchsian subgroups.

In [4] , Fine showed that **P** is a generalised free product and used this fact to characterize Fuchsian subgroups. To do this he needed to find the conjugacy classes of elliptic elements in **P**. In [4] , Fine found five conjugacy classes of elliptic elements of order 2 and two classes of order 3. In [6], Harding noted without proof that the number of conjugacy classes of order 2 can be reduced to four, and used this result in the classification of maximal Fuchsian subgroups of **P**.

In this study, noticing first that the number of conjugacy classes of 3rd order elliptic elements can be reduced to 1, we obtain new results on the subgroups of **P** regarding Harding's results, [6]. Because of the decrease on the number of conjugacy classes, the results obtained in [4] and [6] will become easier to prove and many calculations can be omitted.

An element of $A *_H B$ of finite order is conjugate to an element of finite order in one of the factors. Because of the abstract group structure of **P** as a free product amalgamated with **M**, each finite ordered elliptic element will be either of order 2 or 3. Further P is a discontinuous group and therefore it can not have any elliptic elements of infinite order, [7]. These can be proved by elementary operations. In [4], Fine found the conjugacy classes of elliptic elements of finite order in G_1 and in G_2 to find the conjugacy classes of elliptic elements in **P**. Fine found representatives of the conjugacy classes of elliptic elements of order 2 as

$$z \to -z, z \to \frac{1}{z}, z \to -z+1, z \to -z+i, z \to -z+(1+i).$$

Harding [6], noted that these can be reduced to

$$z \to -z, z \to -z+1, z \to -z+i, z \to -z+(1+i).$$

Indeed by means of the transformation corresponding to the matrix $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, the representatives $z \to \frac{1}{z}$ and $z \to -z+1$ are conjugate. Therefore these elements have exactly four conjugacy classes in $\mathbf{P}$.

Fine, in [4], found the representatives of the conjugacy classes of elliptic elements of order three as $z \to -\frac{1}{z+1}$ and $z \to \frac{1}{z+i}$. But by means of the transformation corresponding to the matrix $\begin{pmatrix} i & -1 \\ -i & 1-i \end{pmatrix}$, these two are conjugate to each other. That is, there is only one class of third order elliptic elements in $\mathbf{P}$. Therefore we can induce the Theorem 2 of [4] to the following.

Theorem 2.1 *There are only five conjugacy classes of elliptic elements in* $\mathbf{P}$*, four for those of order 2 and one for those of order 3. In particular, any elliptic transformation of order 2 is conjugate to one of*

$$\mathfrak{u}_{2,1} : z \to -z, \mathfrak{u}_{2,2} : z \to -z+1, \mathfrak{u}_{2,3} : z \to -z+i, \mathfrak{u}_{2,4} : z \to -z+1+i$$

while any elliptic transformation of order 3 is conjugate to

$$\mathfrak{u}_3 : z \to -\frac{1}{z+1}.$$

Let $\mathfrak{u}_{2,1}$, $\mathfrak{u}_{2,2}$, $\mathfrak{u}_{2,3}$, $\mathfrak{u}_{2,4}$ and $\mathfrak{u}_3$ denote the five conjugacy classes of elliptic elements in $\mathbf{P}$. Before stating our main results, we first give a summary on Hermitian forms and maximal Fuchsian subgroups of $\mathbf{P}$, (for details, see [6] and [8]).

Let C be the circle

$$a(x^2+y^2)+2b_1x-2b_2y+c=0$$

on the complex plane with $a, b_1, b_2, c \in \mathbb{Z}$ and $b_1^2+b_2^2-ac>0$. If we denote the set of those C by Ω, $\mathbf{P}$ acts on Ω.

2.1 Definition *A subgroup of* $\mathbf{P}$ *leaving a circle* C *invariant and mapping its interior onto itself is called Fuchsian.*

We know from [5] that to each circle C of Ω there corresponds a Fuchsian subgroup and to each Fuchsian subgroup there corresponds a circle of Ω.

2.2 Definition *1) A quadratic form* $az\overline{z} + bz + \overline{b}\overline{z} + c$ *is called a binary Hermitian form. Here* $a, c \in \mathbb{Z}$ *and* $b \in \mathbb{Z}(i)$.

If we put $z = x + iy$ *and* $b = b_1 + ib_2$ *, then we obtain* $a(x^2 + y^2) + 2b_1x - 2b_2y + c$. *For brevity, this form can be denoted by* (a, b_1, b_2, c).

2) The discriminant of a form (a, b_1, b_2, c) *is* $D = b_1^2 + b_2^2 - ac$.

Here if $D > 0$, then the form (a, b_1, b_2, c) represents (by putting the form equal to zero) a circle in $\mathbb{C}$ with center $\frac{-b_1+ib_2}{a}$ and radius $\frac{\sqrt{D}}{|a|}$ where $a \neq 0$. When $a = 0$, such a form represents a straight line which is a circle in $\widehat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$.

2.3 Definition *1) Let* C , $C^{'}$ *be any forms. If there exists a* $g \in \mathbf{P}$ *such that* $g(C) = C^{'}$ *then we call these two forms equivalent.*

2) If g.c.d. $(a, b_1, b_2, c) = 1$ *, then the form* (a, b_1, b_2, c) *is called primitive.*

3) The main form of discriminant $D > 0$ *is* $(1, 0, 0, -D)$. *Every main form is primitive and is a circle with centre 0, radius* $\sqrt{D}$.

Equivalent forms have the same discriminant. Let $C, C^{'}$ be represented by (a, b_1, b_2, c) and $(a^{'}, b_1^{'}, b_2^{'}, c^{'})$. Let C, $C^{'}$ be equivalent, i.e. for some $g \in \mathbf{P}$, $g(a, b_1, b_2, c) = (a^{'}, b_1^{'}, b_2^{'}, c^{'})$. Now we consider the presentation of $\mathbf{P}$ in (1.1). $\mathbf{P}$ is generated by the following transformations:

$$x(z) = \frac{i}{iz+1}, u(z) = -\frac{1}{z}, y(z) = \frac{z+1}{-z}, r(z) = \frac{i}{iz}.$$

The effect of x, u, y, r on C can be given

$$\begin{aligned} x &: (a, b_1, b_2, c) \to (a + c - 2b_2, b_1, a - b_2, a) \\ u &: (a, b_1, b_2, c) \to (c, -b_1, b_2, a) \\ y &: (a, b_1, b_2, c) \to (c, c - b_1, b_2, a + c - 2b_1) \\ r &: (a, b_1, b_2, c) \to (c, b_1, -b_2, a) \end{aligned}$$

Then by observation, we have

(i) if at least one of a, c is odd, then at least one of $a^{'}, c^{'}$ is odd.

(ii) if both a, c are even, then both $a^{'}, c^{'}$ are even and $b_i \equiv b_i^{'}(\text{mod}2), i = 1, 2$.

Also by observation, if (a, b_1, b_2, c) and $(a^{'}, b_1^{'}, b_2^{'}, c^{'})$ are both primitive, with the same discriminant, and if they satisfy (i) or (ii), then they are equivalent.So for a given discriminant D, there are (at most) four equivalence classes of primitive forms. They are of the following types:

I) (odd or even, odd or even, odd or even,odd or even) with the condition that a and c can not be even at the same time.

II) (even, odd, odd, even)

III) (even, odd, even, even)

IV) (even, even, odd, even)

Note that the main form of any discriminant is of type I, since $a = 1$ is odd.

2.4 Definition *Let $C = (a, b_1, b_2, c)$ be a form. The subgroup of* **P** *consisting of all transformations leaving C invariant is called the form group (or group) of C and denoted by $\Phi(C)$.*

Here the circle C is left invariant and its interior is mapped onto itself. Therefore a form group $\Phi(C)$ is a maximal Fuchsian subgroup of **P**. The conjugacy classes of maximal Fuchsian subgroups of **P** correspond to equivalence classes of primitive forms in a one to one and onto way.

Theorem 2.2 *Let D be a given determinant.*

If $D \equiv 0(mod4)$, then there is only one equivalence class of primitive forms and is of type I.

If $D \equiv 1(mod4)$, then there are three classes of types I, III and IV.

If $D \equiv 2(mod4)$, then there are two classes, of types I and II.

If $D \equiv 3(mod4)$, then there is only one class of type I.

Proof. (See [6]) We only sketch the proof to remind the method. For all values of discriminant D, there is a main form. So the type I class always exits.

So assume both a, c are even, and so $D \equiv b_1^2 + b_2^2(\text{mod}4)$.

If $D \equiv 0(\text{mod}4)$, we have $b_1^2 + b_2^2 \equiv 0(\text{mod}4)$. Then both b_1, b_2 must be even in which case, form is not primitive. So there is only one class of type I.

If $D \equiv 1(\text{mod}4)$, we have $b_1^2 + b_2^2 \equiv 1 \text{ mod } 4$. In this case b_1 is odd, b_2 is even or vice versa. So there are three classes of type I, III, IV.

The others follow similarly. □

Let us denote the equivalence class of primitive forms of type I having discriminant D by $\xi(I,D)$. Similarly $\xi(II,D)$, $\xi(III,D)$ and $\xi(IV,D)$ denote the equivalence classes of primitive forms of type II, III and IV having discriminant D.

Definition 2.5 *If ξ is an equivalence class of primitive forms and $\mathfrak{u}$ is a conjugacy class of elliptic elements in $\mathbf{P}$, then $\mathfrak{u}$ is said to be represented in ξ if there is an element $b \in \mathfrak{u}$ such that $b \in \Phi(C)$ where $C \in \xi$.*

First, we can restate Theorem 3.7 in [6] as we reduced the number of conjugacy classes of the third order elliptic elements to one.

Theorem 2.3. *Let C be a primitive form.*

(a) *The form group $\Phi(C)$ contains elliptic elements of order 2 conjugate to $\mathfrak{u}_{2,1} : z \to -z$, $\mathfrak{u}_{2,2} : z \to -z+1$, $\mathfrak{u}_{2,3} : z \to -z+i$, $\mathfrak{u}_{2,4} : z \to -z+1+i$, respectively, if and only if C is equivalent to one of the following forms respectively*

(i) $(a,0,0,c)$

(ii) $(a,-\frac{1}{2}a,0,c)$ *a even*

(iii) $(a,0,\frac{1}{2}a,c)$ *a even*

(iv) $(a,-\ \frac{1}{2}a,\frac{1}{2}a,c)$ *a even.*

(b) *$\Phi(C)$ contains elliptic elements of order 3 if and only if C is equivalent to a form $(a,\frac{1}{2}a,b_2,a)$ (a even).*

(c) *$\Phi(C)$ contains parabolic elements if and only if the discriminant of C is in the form $D = dD_0^2$ where, d is square-free and does not have any prime factor $p \equiv 3(mod4)$.*

Proof. **(a)** We know that any elliptic element of order 2 in $\mathbf{P}$ is conjugate to one of the following transformations: $\mathfrak{u}_{2,1} : z \to -z$, $\mathfrak{u}_{2,2} : z \to -z+1$, $\mathfrak{u}_{2,3} : z \to -z+i$, and $\mathfrak{u}_{2,4} : z \to -z+1+i$. Let $C^{'}$ be the form $az\overline{z}+bz+\overline{b}\overline{z}+c$. The transformation $\mathfrak{u}_{2,1} : z \to -z$ sends $C^{'}$ to

$a(-z)(-\overline{z})+b(-z)+\overline{b}(-\overline{z})+c = az\overline{z}-bz-\overline{b}\overline{z}+c.$

This is equal to $C^{'}$ if $b=-b$. So $b=0$ and so $C^{'}$ is of type I. Thus the group of a form equivalent to $C^{'}=(a,0,0,c)$ for some a,c will contain at least one element of order 2 conjugate to $\mathfrak{u}_{2,1} : z \to -z$. Indeed, if a primitive form C is equivalent to $C^{'}$, by the definition, there is an element $g \in P$ such that $g(C)=C^{'}$. Now we consider the element

$g^{-1}\mathfrak{u}_{2,1}g$. As $g^{-1}\mathfrak{u}_{2,1}g(C) = C$ we have $g^{-1}\mathfrak{u}_{2,1}g \in \Phi(C)$. Clearly $g^{-1}\mathfrak{u}_{2,1}g$ is of order 2. So $\Phi(C)$ contains elliptic elements of order 2 conjugate to $\mathfrak{u}_{2,1} : z \to -z$.

The transformation $\mathfrak{u}_{2,2} : z \to -z+1$ sends $C^{'}$ to $a(-z+1)(-\overline{z}+1) + b(-z+1) + \overline{b}(-\overline{z}+1) + c = az\overline{z} + (-a-b)z + (-a-\overline{b})\overline{z} + a + b + \overline{b} + c$. This is $C^{'}$ if $b = -a-b$, $a + b + \overline{b} + c = c$. So $2b_1 = -a, b_2 = 0$ where $b = b_1 + ib_2$. Thus the group of a form equivalent to $C^{'} = (a, -\frac{1}{2}a, 0, c)$ for some a (even) and c will contain at least one element of order 2 conjugate to $\mathfrak{u}_{2,2} : z \to -z+1$. The form will be of type I or III according to whether c is odd or even.

Similarly, the group of a form equivalent to $C^{'} = (a, 0, \frac{1}{2}a, c)$ for some a (even) and c will contain at least one element conjugate to $\mathfrak{u}_{2,3} : z \to -z+i$. The form will be of type I or IV according to whether c is odd or even.

Similarly, the group of a form equivalent to $C^{'} = (a, -\frac{1}{2}a, \frac{1}{2}a, c)$ for some a (even) and c will contain at least one element conjugate to $\mathfrak{u}_{2,4} : z \to -z+1+i$. The form will be of type I or II.

Conversely, assume that $\Phi(C)$ contains an elliptic element of order 2 conjugate to $\mathfrak{u}_{2,2} : z \to -z+1$, say a. Since a is conjugate to $\mathfrak{u}_{2,2}$ in $\mathbf{P}$, by the definition there is an element b of $\mathbf{P}$ such that $bab^{-1} = \mathfrak{u}_{2,2}$. Now we consider the circle $C^{'} = b(C)$. Since $\mathfrak{u}_{2,2}(C^{'}) = bab^{-1}(C^{'}) = C^{'}$, we have $\mathfrak{u}_{2,2} \in \Phi(C^{'})$. Therefore, we have seen that, if $\mathfrak{u}_{2,2} \in \Phi(C^{'})$ then $C^{'}$ is of the form $(a, -\frac{1}{2}a, 0, c)$ (a even). By the definition, as $b(C) = C^{'}$, C is equivalent to $C^{'} = (a, -\frac{1}{2}a, 0, c)$ (a even).

The others follow similarly.

(b) Let $C^{'}$ be the form $az\overline{z} + bz + \overline{b}\overline{z} + c$. We know that any elliptic element of order 3 in $\mathbf{P}$ is conjugate to $\mathfrak{u}_3 : z \to \frac{-1}{z+1}$. The transformation $\mathfrak{u}_3 : z \to \frac{-1}{z+1}$ sends $C^{'}$ to

$$a(\tfrac{-1-z}{z})(\tfrac{-1-\overline{z}}{\overline{z}}) + b\tfrac{-1-z}{z} + \overline{b}\tfrac{-1-\overline{z}}{\overline{z}} + c = a(1+z)(1+\overline{z}) - b(1+z)\overline{z} - \overline{b}(1+\overline{z})z + cz\overline{z}$$
$$= (a - b - \overline{b} + c)z\overline{z} + (a-\overline{b})z + (a-b)\overline{z} + a.$$

This is equal to $C^{'}$ if $a = c$ and $b = a - \overline{b}$. So we have $a = c$ and $2b_1 = a$ where $b = b_1 + ib_2$. Therefore if $\mathfrak{u}_3 \in \Phi(C^{'})$ then C$^{'}$ must be of the form $(a, \frac{1}{2}a, b_2, a)$ for some a (even) and b. The form will be of type II, III or IV according to whether $a, \frac{1}{2}a$ and b_2 are odd or even. Thus the group of a form equivalent to $C^{'} = (a, \frac{1}{2}a, b_2, a)$ for some a (even) and b will contain at least one element of order 3. Indeed, if a primitive form C is equivalent to $C^{'}$, by the definition, there is an element $g \in \mathbf{P}$ such that $g(C) = C^{'}$. Now we consider the element $g^{-1}\mathfrak{u}_3 g$. As $g^{-1}\mathfrak{u}_3 g(C) = C$ we have $g^{-1}\mathfrak{u}_3 g \in \Phi(C)$. Clearly

$g^{-1}\mathfrak{u}_3 g$ is of order 3. So $\Phi(C)$ contains elliptic elements of order 3.

Conversely, assume that $\Phi(C)$ contains an elliptic element of order 3, say a. Since any elliptic element of order 3 in $\mathbf{P}$ is conjugate to $\mathfrak{u}_3 : z \to \frac{-1}{z+1}$, a is conjugate to $\mathfrak{u}_3$. By the definition there is an element b of $\mathbf{P}$ such that $bab^{-1} = \mathfrak{u}_3$. Now we consider the circle $C^{'} = b(C)$. Since $\mathfrak{u}_3(C^{'}) = bab^{-1}(C^{'}) = C^{'}$, we have $\mathfrak{u}_3 \in \Phi(C^{'})$. We have seen that, if $\mathfrak{u}_3 \in \Phi(C^{'})$ then $C^{'}$ is of the form $(a, \frac{1}{2}a, b_2, a)$ for some a (even) and b. As $b(C) = C^{'}$, by the definition, C is equivalent to $C^{'} = (a, \frac{1}{2}a, b_2, a)$ (a even).

(c) Follows similarly. □

Then we have the following theorem.

Theorem 2.4 *$\mathfrak{U}_{2,1}$ is represented in $\xi(I)$ for all values of D. $\mathfrak{u}_3$ can not be represented in $\xi(I)$ for all values of D. If $D \equiv 1(mod4)$, only $\mathfrak{U}_{2,2}$ is represented in $\xi(III)$ and only $\mathfrak{U}_{2,3}$ is represented in $\xi(IV)$. Also, if $D \equiv 2(mod4)$, only $\mathfrak{U}_{2,4}$ is represented in $\xi(II)$.*

Proof. Let D be any discriminant. For every D, there is the type I class and we take the main form $C_1 = (1, 0, 0, -D)$ as its representative. So by the Theorem 2.3(a)(i), $\Phi(C_1)$ contain $\mathfrak{u}_{2,1}$. Then for $\mathfrak{u}_{2,1} \in \mathfrak{u}_{2,1}$, $\mathfrak{u}_{2,1} \in \Phi(C_1)$ where $C_1 \in \xi(I, D)$. Thus $\mathfrak{u}_{2,1}$ is represented in $\xi(I, D)$ for any D.

Now suppose that $\mathfrak{u}_3$ is represented in $\xi(I, D)$ for any D. By the definition, there is an element $b \in \mathfrak{u}_3$ such that $b \in \Phi(C)$ where $C \in \xi(I, D)$. As $b \in \mathfrak{u}_3$, there is a $y \in \mathbf{P}$ such that $yby^{-1} = \mathfrak{u}_3$. Then we have $\mathfrak{u}_3\,(y(C)) = y(C)$. By the Theorem 2.3(b), $y(C)$ must be of the form $(a, \frac{1}{2}a, b_2, a)$ for some a (even), b. By the definition C and $y(C)$ are equivalent. But $y(C) = (a, \frac{1}{2}a, b_2, a)$ is not of type I. Because of this contradiction, $\mathfrak{u}_3$ can not be represented in $\xi(I, D)$ for any D.

By the Theorem 2.2, we know that for $D \equiv 0, 3(\text{mod}4)$ there is only type I. Therefore only $\mathfrak{u}_{2,1}$ is represented in $\xi(I, D)$ for this values of D. If $D \equiv 1(\text{mod}4)$, there are three classes of type I, III and IV. Then

$$C_3 : 2z\overline{z} - z - \overline{z} - (\frac{D-1}{2}) = 0$$

is in $\xi(III, D)$ and

$$C_4 : 2z\overline{z} + iz - i\overline{z} - (\frac{D-1}{2}) = 0$$

is in $\xi(IV, D)$. So by Theorem 2.3(a)(ii) and (iii), $\mathfrak{u}_{2,2} \in \Phi(C_3)$ and $\mathfrak{u}_{2,3} \in \Phi(C_4)$. Therefore $\mathfrak{u}_{2,2}$ is represented in $\xi(III, D)$ and $\mathfrak{u}_{2,3}$ is represented in $\xi(IV, D)$ for all $D \equiv 1(\text{mod}4)$.

Similarly if $D \equiv 2(\text{mod}4)$, there are two classes of type I and II. Then

$$C_2 : 2z\overline{z} + (-1+i)z + (-1-i)\overline{z} - (\frac{D-2}{2}) = 0$$

is in $\xi(II, D)$ and $\mathfrak{u}_{2,4} \in \Phi(C_2)$. Therefore $\mathfrak{u}_{2,4}$ is represented in $\xi(II, D)$ for all $D \equiv 2(\text{mod}4)$. □

Consequently, $\mathfrak{u}_3$ can not be represented in $\xi(I, D)$ for any values of D. Therefore we face the question that for what D's, $\mathfrak{u}_3$ is represented in $\xi(II, D)$, $\xi(III, D)$ and $\xi(IV, D)$.

Theorem 2.5 *Let D be a given discriminant. If $\mathfrak{u}_3$ is represented in $\xi(II, D)$, $\xi(III, D)$ or $\xi(IV, D)$, then there is an $n \in \mathbb{Z}$ so that $D + 3n^2$ is a square.*

Proof. If $\mathfrak{U}_3$ is represented in $\xi(II, D)$, there is an element $b \in \mathfrak{u}_3$ such that $b \in \Phi(C)$ where $C \in \xi(II, D)$. If $b \in \mathfrak{u}_3$, there is a $g \in \mathbf{P}$ so that $gbg^{-1} = \mathfrak{u}_3$. Then we have $\mathfrak{u}_3\,(g(C)) = g(C)$. By Theorem 2.3(b), $g(C)$ is of the form $(a, \frac{1}{2}a, b_2, a)$ with even a. Therefore C is equivalent to a form $(a, \frac{1}{2}a, b_2, a)$ with even a. Since equivalent forms have equal discriminant, we get $D = \frac{a^2}{4} + b_2^2 - a^2$ and so $b_2^2 = D + 3\frac{a^2}{4}$. As a is even, we write $a = 2n, n \in \mathbb{Z}$. Then $b_2^2 = D + 3n^2$ and hence $b_2 = \sqrt{D + 3n^2}$ is obtained. Since $b_2 \in \mathbb{Z}$, we conclude that $D + 3n^2$ is an exact square. The others follows similarly. □

If $D + 3n^2 = a^2$, then the form $(2n, n, a, 2n)$ is of the type II, III or IV with discriminant D according to whether n and a are odd or even. If $(n, a) = 1$, the form $(2n, n, a, 2n)$ will be primitive. In other words, if $D + 3n^2 = a^2$ with $(n, a) = 1$, then $\mathfrak{u}_3$ is represented in $\xi(II, D)$, $\xi(III, D)$ or $\xi(IV, D)$.

The converse of this theorem is not always true, e.g. for $D = 9$, we find $9 + 3.3^2 = 36$ and the corresponding form $(6, 3, 6, 6)$ is not primitive.

Let $D + 3n^2 = a^2$. Suppose that n and a are both even. Then we can write $a = 2m$, $n = 2u$ where $m, u \in \mathbb{Z}$. We have $D = a^2 - 3n^2 = 4m^2 - 12u^2 \equiv 0(\text{mod}4)$. If n is odd and a is even, we have $D = (2m)^2 - 3(2u+1)^2 = 4(m^2 - 3u^2 - 3u - 1) + 1 \equiv 1(\text{mod}4)$. Similarly, if n is even and a is odd, we have $D \equiv 1(\text{mod}4)$. Finally if n and a are both odd, we have $D \equiv 2(\text{mod}4)$. Thus we have the following lemma:

Lemma 2.6 *(i) Let $D \equiv 2(mod 4)$ and $D+3n^2=a^2$. Then a and n are both odd.*

(ii) Let $D \equiv 1(mod 4)$ and $D+3n^2=a^2$. Then n is odd while a is even and vice versa.

Therefore if $D+3n^2=a^2$ with $(n,a)=1$ and $D \equiv 2(\text{mod}4)$, then the form $(2n,n,a,2n)$ is a representative of forms of type II having discriminant D. So $\mathfrak{u}_3$ is represented in $\xi(II,D)$ for the values of D. If $D+3n^2=a^2$ with $(n,a)=1$ and $D \equiv 1(\text{mod}4)$, then the forms $(2n,n,a,2n)$ and $(4n+2a,2n+a,3n+2a,4n+2a)$ are representatives of forms of type III and IV having discriminant D according to whether n and a are odd or even. Notice that the parity of the pair (n,a) is opposite to that of the pair $(2n+a,3n+2a)$. So $\mathfrak{u}_3$ is represented in $\xi(III,D)$ and $\xi(IV,D)$ for the values of D.

Now we want to determine what values of $D \equiv 1,2(\text{mod}4)$, the positive integer D can be represented in the quadratic form $D=a^2-3n^2$ by integers a,n where $(n,a)=1$. First we will solve the problem for $n=1$ and 2. Note that for $n=0$, only possible case is $a=1$ and we have $D=1$. First assume that $n=1$. If a is odd, we can write $a=2u+1, u\in\mathbb{Z}$. Then we have $D=a^2-3=4u^2+4u-2\equiv 2(\text{mod}4)$. As $D>0$, all the numbers $D\equiv 2(\text{mod}4)$ with $D+3=a^2$ are of the form

$$D=4u^2+4u-2, u\geq 1.$$

So for these values of D, $\mathfrak{u}_3$ can be represented in $\xi(II,D)$. If a is even, we have $D=4u^2-3\equiv 1(\text{mod}4), u\geq 1$. So all the numbers $D\equiv 1(\text{mod}4)$ with $D+3=a^2$ are of the form

$$D=4u^2-3, u\geq 1$$

and for these values of D, $\mathfrak{u}_3$ can be represented in $\xi(III,D)$ and $\xi(IV,D)$.

Similarly for $n=2$, only the case odd a is possible. Notice that for all odd a, we have $(2,a)=1$. Then we have

$$D=4u^2+4u-11, u\geq 2.$$

So $D\equiv 1(\text{mod}4)$ and these values of D only ones with $D+12=a^2, (2,a)=1$. Again, for these values of D, $\mathfrak{u}_3$ can be represented in $\xi(III,D)$ and $\xi(IV,D)$.

In general, let us consider the binary quadratic form in two variables $f(x,y)=x^2-3y^2$. The standard method of determining which integers can be represented by a quadratic form is to use a local global approach (see, for example, Theorem 1.3 on page 129 in [3]). For the quadratic form under consideration this says:

$x^2 - 3y^2 = D$ $(D > 0)$ has a solution in $\mathbb{Z}$ if and only if $x^2 - 3y^2 = D$ has a solution in $\mathbb{Z}_p$ for each prime p (here $\mathbb{Z}_p$ is the ring of p-adic integers). Furthermore, for odd p, $x^2 - 3y^2 = D$ has a solution in $\mathbb{Z}_p$ if and only if the congruence $x^2 - 3y^2 \equiv D \pmod{p}$ has a solution. For $p = 2$, a similar result holds so long as the corresponding congruence $(\bmod 8)$ is satisfied.

Let $D \equiv 1 (\bmod 4)$.

Case 1. Let $(D, 3) = 1$.

(i) If p is an odd prime, $p \neq 3$, $(D, p) = 1$, then $x^2 - 3y^2 \equiv D \pmod{p}$ always has a solution.

(ii) If p is an odd prime, $p \neq 3$, $p \mid D$, then $x^2 - 3y^2 \equiv D \pmod{p}$ has a solution if and only if $\left(\frac{3}{p}\right) = 1$, i.e. if and only if $p \equiv \pm 1 (\bmod 12)$.

(iii) If $p = 3$, then $x^2 - 3y^2 \equiv D \pmod{3}$ has a solution if and only if $\left(\frac{D}{3}\right) = 1$, i.e. if and only if $D \equiv 1 (\bmod 3)$.

(iv) If $p = 2$, then $x^2 - 3y^2 \equiv D \pmod{8}$ has a solution since $D \equiv 1 (\bmod 4)$ and so $D \equiv 1, 5 (\bmod 8)$.

Therefore we get

" If $D \equiv 1 (\bmod 4)$ and $(D, 3) = 1$, then $x^2 - 3y^2 = D$ has a solution if and only if $D \equiv 1 (\bmod 12)$ and every prime $p \mid D$ is such that $p \equiv \pm 1 (\bmod 12)$."

Case 2. Let $3 \mid D$. This then forces $3 \mid x$ and since $(x, y) = 1$, we must have that 9 does not divide D. Thus $D = 3E$ where $(E, 3) = 1$ and we need to consider solutions to $3x^2 - y^2 = E$.

(i) If p is an odd prime, $p \neq 3, (p, E) = 1$, then there is a solution.

(ii) If p is an odd prime, $p \neq 3$, $p \mid E$, then there is a solution if and only if $p \equiv \pm 1 (\bmod 12)$.

(iii) If $p = 3$, then there is a solution if and only if $E \equiv -1 (\bmod 3)$.

(iv) If $p = 2$, then there is a solution since $E \equiv 3, 7 (\bmod 8)$.

Therefore we get

" If $D \equiv 1 (\bmod 4)$ and $3 \mid D$, then $x^2 - 3y^2 = D$ has a solution if and only if $D \equiv -3 (\bmod 36)$ and every prime $p \mid D, (p \neq 3)$ is such that $p \equiv \pm 1 (\bmod 12)$."

Let $D \equiv 2 (\bmod 4)$. Similarly we get

1. If $D \equiv 2 (\bmod 4)$ and $(D, 3) = 1$, then $x^2 - 3y^2 = D$ has a solution if and only if $D \equiv 10 (\bmod 12)$ and every prime $p \mid D, (p \neq 2)$ is such that $p \equiv \pm 1 (\bmod 12)$.

2. If $D \equiv 2(\text{mod}4)$ and $3 \mid D$, then $x^2 - 3y^2 = D$ has a solution if and only if $D \equiv 6(\text{mod}36)$ and every prime $p \mid D, (p \neq 2, 3)$ is such that $p \equiv \pm 1(\text{mod}12)$.

So we proved the following theorem:

Theorem 2.7. *(i) If $D \equiv 1(mod12)$, and every prime $p \mid D$ is such that $p \equiv \pm 1(mod12)$,*

(ii) If $D \equiv -3(mod36)$, and every prime $p \mid D, (p \neq 3)$ is such that $p \equiv \pm 1(mod12)$,

(iii) If $D \equiv 10(mod12)$, and every prime $p \mid D, (p \neq 2)$ is such that $p \equiv \pm 1(mod12)$,

(iv) If $D \equiv 6(mod36)$, and every prime $p \mid D, (p \neq 2, 3)$ is such that $p \equiv \pm 1(mod12)$,

then $\mathfrak{U}_3$ can be represented in $\xi(II, D)$, $\xi(III, D)$ and $\xi(IV, D)$.

Acknowledgment

We would like to thank the referee for many helpful comments and suggestions. Also, we would like to thank Prof. Dr. Aydın Aytuna.

References

[1] A.F. Beardon, *The Geometry of Discrete Groups*, Graduate Texts in Mathematics 91, Springer-Verlag, New York (1983).

[2] A.M. Brunner, *A Two-Generator Presentation for the Picard Group*, Proc. of the Amer. Math. Soc., Vol.115, Number 1 (1992), 45-46.

[3] J.W.S. Cassels, *Rational Quadratic Forms*, Academic Press (1978).

[4] B. Fine, *Fuchsian Subgroups of the Picard Group*, Canad. J. Math. 28 (1976), 481-485.

[5] R. Fricke and F. Klein, *Volesungen über die Theorie der Automorphen Funktionen*, Vol.I, Teubner Reprint, Leipzig (1965).

[6] S. Harding, *Some Arithmetic and Geometric Problems Concerning Discrete Groups*, Ph.D. Thesis, Univ. of Southampton (1985).

[7] J. Lehner, *Discontinuous Groups and Automorphic Functions*, Math. Surveys No.8, Amer. Math. Soc. (1964).

[8] C. Maclachlan and A.W. Reid, *Parametrizing Fuchsian Subgroups of the Bianchi Groups*, Canad. J. Math., 43 (1991), 158-181.

Nihal YILMAZ, İ. Naci CANGÜL
Received 28.01.1999
Uludağ University, Faculty of Science,
Department of Mathematics
16059, Bursa-TURKEY