Novi Sad J. Math.
Vol. 42, No. 2, 2012, 133-143

MODULAR GROUP ACTION ON QUADRATIC FIELD BY LINEAR CONGRUENCE

Farkhanda Afzal[1], **Qamar Afzal**[2] **and M Aslam Malik**[3]

Abstract. This paper illustrates the Mobius groups M and M' on $Q(\sqrt{m})$, where $M' = \langle xy, yx\rangle$ is a subgroup of M. The system of linear congruence is used to discover classes $[a, b, c](mod12)$ of elements of $Q^*(\sqrt{n})$ and then by means of these classes, we explored several M'-subsets of $Q'''(\sqrt{n})$ which assist in finding more *M-subsets* of $Q(\sqrt{m})$.

AMS Mathematics Subject Classification (2010): 05C25, 11E04, 20G15

Key words and phrases: Möbius Groups, Real Quadratic Irrational Numbers, Linear Congruence, Linear Fractional Transformations, M-subsets

1. Introduction

There is a dictum that anyone who desires to get at the root of a topic should first study its history. That is why in this section we have thrown light on some known results from the previous work done in this area of mathematics. We believe that by this approach, readers will be able to support the parts that they find most difficult. We have embodied the background material about the action of Möbius groups on the real quadratic fields (Q$\sqrt{m}$).

Möbius groups have always attracted great attention in finding group actions on quadratic fields. G. Higman familiarized coset diagrams for presenting the action of modular groups onto number fields.

Q. Mushtaq laid the foundation and established it further. Higman et al. [3] proved that the group PSL(2,Z) is generated by the linear fractional transformations

$$x'(z) = \frac{1}{-z} \text{ and } y'(z) = \frac{z-1}{z}$$

Q. Mushtaq proved that every real quadratic irrational number can be represented uniquely as $\frac{a+\sqrt{n}}{c}$ with a non-square positive integer n, where $a, \frac{a^2-n}{c}$ and c are relatively prime integers [17]. He also discovered that the ambiguous numbers in $Q^*(\sqrt{n})$ are finite and that part of the coset diagram containing these numbers forms a single closed path under the action of G and the set is invariant under the action of G, [18].

[1]School of Mathematics and System Sciences, Beihang University, Beijing, China, e-mail: farkhanda_imran@live.com

[2]Faculty of Mathematics, University of Education, Kalsoom Campus Okara, Pakistan, e-mail: qamarafzal.edu@gmail.com

[3]Faculty of Mathematics, University of the Punjab, New Campus, Lahore, Pakistan, e-mail: aslam.math@pu.edu.pk

In 1989, Mushtaq [19] investigated the extended modular group acting on the projective line over a Galois field. Mushtaq and Shaheen [20] showed some special circuits in coset diagrams, while Mushtaq et al. discussed the group generated by two elements of orders 2 and 4 acting on real quadratic field in [21].

Aslam Malik et al. [7] studied modular group action on certain quadratic fields. In [8] the authors proved that the action of G on $Q^*(\sqrt{n})$ for $n \neq 2$, is intransitive. Imrana Kouser et al. in [4] gave a classification of the elements $\frac{a+\sqrt{p}}{c}$ of $Q^*(\sqrt{p})$ with respect to odd/even nature of a, b and c. They have obtained a classification of $Q^*(\sqrt{p})$ and a partition of $Q^*(\sqrt{p})$ under the modular group $PSL(2, Z)$ as well. In [12] Aslam Malik et al. discussed the properties of real quadratic irrational numbers under the action of the group $H = \langle x, y : x^2 = y^4 = 1\rangle$.

In [5] M. Ashiq studied an action of two-generator groups on a real quadratic field. Ashiq and Mushtaq [6] investigated the action of a subgroup of a modular group on an imaginary quadratic field. The imaginary quadratic fields are defined as $Q(\sqrt{-m}) = \{a + b\sqrt{-m}; a, b \in Q\}$, where m is a square free positive integer. They proved that the action of a subgroup of G on $Q(\sqrt{-m})$ is always transitive. They have also proved [16] that the action of M on $Q(\sqrt{m})$ is intransitive for $m = 3k$ and $m = 3k + 1$.

Aslam [15] studied the action of $\langle y, t : y^4 = t^4 = 1\rangle$ on $Q(\sqrt{m})$. By using the coset diagram for the action of $H = \langle y, t : y^4 = t^4 = 1\rangle$ on $Q(\sqrt{m})$, they showed that if α is of the form $\frac{\alpha+\sqrt{n}}{2c}$, then every element in the orbit αH is also of the form $\frac{\alpha'+\sqrt{n}}{2c'}$ and $\alpha H \subset Q^*(\sqrt{n})$.

M Aslam Malik et al. [9] generalized these results by using the notion of congruence. They have proved that for each square free positive integer $n > 2$, the action of group G on $Q^*(\sqrt{n})$ is intransitive. They also discussed some properties of real quadratic irrational numbers under the action of $M = \langle x, y : x^2 = y^6 = 1\rangle$ in [10] and [11]. Mehmood has proved that there exist two G-subsets of $Q^*(\sqrt{n})$ if n is a quadratic residue [13]. Zafar [14] obtained two proper G-subsets of $Q^*(\sqrt{n})$ corresponding to each odd prime divisor of n. In [2] we have given a classification of the real quadratic irrational numbers $\frac{a+\sqrt{n}}{c}$ of $Q^*(\sqrt{n})$ with respect to modulo 3^r.

Our interest is to find linear transformation in general x,y satisfying the relations $x^2 = y^m = 1$, with a view to studying the action of the group $\langle x, y\rangle$ on real quadratic fields. We are interested in the group $\langle x, y\rangle$ for $m = 6$. That is $M = \langle x, y; x^2 = y^6 = 1\rangle$. We find a proper subgroup $M' = \langle xy, yx\rangle$ of M which is very much useful in finding M-subsets. This paper describes the actions of Möbius groups M and M' on real quadratic fields. Here we find M'-subsets which facilitate the finding of M-subsets with the assistance of congruence classes. Also, by using the system of linear congruence we find the classes $[a, b, c](mod 12)$ of elements of $Q^*(\sqrt{n})$ and then we investigate more M'-subsets of $Q'''(\sqrt{n})$.

2. Preliminaries

Möbius transformation or map is a function f of a complex variable z that can be written in the form $f(z) = \frac{az+b}{cz+d}$; for some complex numbers a, b, c and d with $ad - bc \neq 0$. The set of all Möbius transformation forms a group under composition called the Möbius group. The Möbius group M is defined as $M = \langle x, y; x^2 = y^6 = 1\rangle$, where $x(\alpha) = \frac{-1}{3}$ and $y(\alpha) = \frac{-1}{3(\alpha+1)}$ are linear fractional transformations. Throughout this paper we take m as a square free positive integer. An element $a + b\sqrt{m}$, $b \neq 0$, of real quadratic field $Q\sqrt{m} = \{a + b\sqrt{m} : a, b \in Q\}$ is called a real quadratic irrational number. A set X with some action on group G on it, is known as G-set. A subset X' of G-sets is called a G-subset if $g \in G \Rightarrow a^g \in X'$ for each $a \in X'$.

If $n = k^2m$ and $k > 0$ be an integer, then we have the following definitions:

$$\begin{aligned} Q^*(\sqrt{n}) :=& \{\frac{a+\sqrt{n}}{c} : a, b := \frac{a^2-n}{c}, c \in Z \text{ and } (a, \frac{a^2-n}{c}, c) = 1\} \\ Q'''(\sqrt{n}) =& \{\alpha/t; \alpha \in Q^*(\sqrt{n}); t = 1, 3\} \\ Q^{***}(\sqrt{n}) =& \{\frac{(a+\sqrt{n})}{c} \in Q^*(\sqrt{n}) : 3|c\}. \end{aligned}$$

Lemma 2.1. *[10] Let n be a non-square positive integer, $\alpha \in Q^*(\sqrt{n})$ with $b = \frac{a^2-n}{c}$, then*

1. *If $n \not\equiv 0(mod 9)$, then $\frac{\alpha}{3}$ belongs to $Q^*(\sqrt{n})$ if and only if $3|b$*
2. *$\frac{\alpha}{3}$ belongs to $Q^*(\sqrt{9n})$ if and only if $3 \nmid b$.*

Our first lemma produces that if $\frac{a+\sqrt{n}}{c} \in Q^{***}(\sqrt{n})$ with $n \equiv 0(mod 3)$then $a \equiv 0(mod 3)$.

Lemma 2.2. *Let $\frac{a+\sqrt{n}}{c} \in Q^{***}(\sqrt{n})$ with $n \equiv 0(mod 3)$, then there must be $a \equiv (mod 3)$ only.*

Proof. As we know $a^2 - bc \equiv n(mod 3)$. Thus $a^2 \equiv bc + n(mod 3)$. So $a^2 \equiv 0(mod 3)$ since $c \equiv 0(mod 3)$ for all $\frac{a+\sqrt{n}}{c} \in Q^{***}(\sqrt{n})$. Hence $a \equiv 0(mod 3)$. □

3. Subgroups of M and M-subsets

Now we present the idea of subgroups of M and explore the action of some important subgroups of M on $Q(\sqrt{m})$. Since M is a finitely generated group then it contains infinitely many two-generator subgroups. Let $M' = \langle u, v\rangle$, where $u = xy$ and $v = yx$ are linear fractional transformations $u : \alpha \to \alpha + 1$ and $v : \alpha \to \frac{\alpha}{1-3\alpha}$. It is easy to see that $u^n = \alpha + n$ and $v^n = \frac{\alpha}{1-3n(\alpha)}$; $n = 1, 2, \ldots$. These equations imply that u, v are of infinite order. Since each $g \in M'$ is a word in xy, yx, y^2, and y^4. Therefore u, v, (vu), $u(vu)$, $u(vu)^2$, $(vu)v$ and $(vu)^2$ are important elements of M'. We have the following important results obtained after the actions of Möbius group M' on real quadratic fields.

Theorem 3.1. *Let $xy = u$ and $yx = v$ and $M' = \langle u, v\rangle$, then for any non-square positive integer n, the sets:*

$$A = \{\frac{a+\sqrt{n}}{c} \in Q^*(\sqrt{n}) : c \equiv 1(mod 3)\}$$

and

$$B = \{\frac{a+\sqrt{n}}{c} \in Q^*(\sqrt{n}) : c \equiv 2(mod3)\}$$

are M'-subset.

Proof. Since $n \equiv 0, 1$ or $2(mod3)$, so we discuss these cases separately.

In the first case let $n \equiv 0mod3$.

Let $\frac{a+\sqrt{n}}{c} \in A$. We know that $a^2 - bc \equiv n(mod3)$, then

$$a^2 - bc \equiv 0(mod3) \Rightarrow a^2 \equiv bc(mod3) \Rightarrow a^2 \equiv b(mod3),$$

since $c \equiv 1(mod3)$.

Now $a \equiv 0, 1$ or $2(mod3)$, therefore $a^2 \equiv 0$ or $1(mod3)$ as $a^2 \equiv 0(mod3)$ if $a \equiv 0(mod3)$ and $a^2 \equiv 1(mod3)$ if $a \equiv 1, 2(mod3)$.

If $a^2 \equiv 0(mod3)$ then $b \equiv 0(mod3)$ and if $a^2 \equiv 1(mod3)$, then $b \equiv 1(mod3)$. Thus $A = \{\frac{a+\sqrt{n}}{c} \in Q^*(\sqrt{n}) : c \equiv 1(mod3)\}$ consists of elements of the forms $[0, 0, 1]$, $[1, 1, 1]$ and $[2, 1, 1]$ only.

Let $\frac{a+\sqrt{n}}{c} \in B$, then $a^2 - bc \equiv n(mod3) \Rightarrow a^2 \equiv bc(mod3)$ therefore $n \equiv 0(mod3)$, since $c \equiv 2(mod3)$ given, then $a^2 \equiv 2b(mod3)$. If $a \equiv 0(mod3)$, then $a^2 \equiv 0(mod3)$ and hence $b \equiv 0(mod3)$. Similarly, if $a \equiv 1$ or $2(mod3)$, then $a^2 \equiv 1(mod3)$ and hence $b \equiv 2(mod3)$. Similarly, if $a \equiv 1$ or $2(mod3)$, then $a^2 \equiv 1(mod3)$ and hence $b \equiv 2mod3$.

Since $a^2 \equiv 2b(mod3)$. Thus the elements in set $B = \{\frac{a+\sqrt{n}}{c}; \alpha \in Q^*(\sqrt{n}) : c \equiv 2(mod3)\}$ are of the forms $[0, 0, 2]$, $[1, 2, 2]$ and $[2, 2, 2]$ only. Hence every element of M' is a word in the generator u, v of M'. Thus it is enough to show that elements of the sets A and B are mapped on A and B respectively under u and v. We know

$$xy(\frac{a+\sqrt{n}}{c}) = \frac{(a+c)+\sqrt{n}}{c} = \frac{a_1+\sqrt{n}}{c_1}; a_1 = a+c, b_1 = 2a+b+c, c_1 = c.$$

$$yx(\frac{a+\sqrt{n}}{c}) = \frac{(a-3b)+\sqrt{n}}{-6a+9b+c} = \frac{a_2+\sqrt{n}}{c_2}; a_2 = a-3b, 2 = b, c_2 = -6a+9b+c.$$

Thus u takes elements of the forms $[0, 0, 1]$, $[1, 1, 1]$, and $[2, 1, 1]$ onto elements of the forms $[1, 1, 1]$, $[2, 1, 1]$ and $[0, 0, 1]$ respectively. Also $[0, 0, 1]$, $[1, 1, 1]$ and $[2, 1, 1]$ maps onto elements of the forms $[0, 0, 1]$, $[1, 1, 1]$ and $[2, 1, 1]$ respectively under v. Thus the elements of A are mapped on to the elements of the forms $[0, 0, 1]$, $[1, 1, 1]$ and $[2, 1, 1]$. Therefore, the set A is a M'-subset.

Similarly, it can be checked that the elements of B of the forms $[0, 0, 2]$, $[1, 2, 2]$ and $[2, 2, 2]$ are mapped onto $[0, 0, 2]$, $[1, 2, 2]$ and $[2, 2, 2]$ under u and v. Thus A and B are M'-subset. Similarly, one can easily check A and B for other two cases that is $n \equiv 1(mod3)$ and $n \equiv 2(mod3)$. □

The above theorem deals with the case when $c \equiv 1$ or $2(mod3)$. The question arises as to the cases when $c \equiv 0(mod3)$. These cases do not arise when $n \equiv 2(mod3)$. Therefore we will discuss this for the remaining two cases. The following theorem deals with the case when $n \equiv 1(mod3)$.

Theorem 3.2. *Let $n \equiv 1(mod3)$ be a non-square positive integer, then*

$$A = \{\frac{a+\sqrt{n}}{c}; \alpha \in Q^{***}(\sqrt{n}) : a \equiv 1(mod3)\}$$

$$B = \{\frac{a+\sqrt{n}}{c}; \alpha \in Q^{***}(\sqrt{n}) : a \equiv 2(mod3)\}$$

are both M'-subsets.

Proof. Consider $n \equiv 1(mod3)$.

Let $\alpha = \{\frac{\alpha+\sqrt{n}}{c} \in Q^{***}(\sqrt{n}) : c \equiv 0(mod3)\}$ and since $a^2 - bc \equiv n(mod3)$, then $a^2 \equiv bc(mod3)$ since $c \equiv 0(mod3)$ and $n \equiv 1(mod3)$, hence $b \equiv 0, 1$ or $2(mod3)$. Now $a^2 \equiv 1(mod3)$ implies $a \equiv 1$ or $2(mod3)$. So the elements of the set A are of the forms $[1, 1, 0]$, $[1, 0, 0]$,$[1, 2, 0]$ only, and the set B consists of elements of the forms $[2, 1, 0]$, $[2, 0, 0]$ and $[2, 2, 0]$ only.

Thus it can be verified that the elements of the set A are mapped onto the elements of the forms $[1, 0, 0]$, $[1, 2, 0]$ and $[1, 1, 0]$ under the actions of u,$v \in M'$. Also, the elements of the set B are mapped onto elements of the forms $[2, 1, 0]$, $[2, 0, 0]$ and $[2, 2, 0]$ under the action of M'. Hence, A and B are M'-subsets of $Q^{***}(\sqrt{n})$. □

In the next theorem we consider the case when $n \equiv 0(mod3)$. This provides us two M'-subsets of $Q^{***}(\sqrt{n})$.

Theorem 3.3. *Let $n \equiv 0(mod3)$ be a non-square positive integer, then the sets*

$$A = \{\frac{a+\sqrt{n}}{c}; \alpha \in Q^{***}(\sqrt{n}) : b \equiv 1(mod3)\}$$

$$B = \{\frac{a+\sqrt{n}}{c}; \alpha \in Q^{***}(\sqrt{n}) : b \equiv 2(mod3)\}$$

are M'-subsets of $Q'''(\sqrt{n})$

Note that each $n \equiv 0(mod3)$ gives rise to three cases $n \equiv 0, 3or6(mod9)$. Then, the above theorem leads to the following corollary.

Corollary 3.1. *Let n be a non-square positive integer such that $n \equiv 3(mod9)$. Then the sets A and B of Theorem 3.3 become*

$$A = \{\frac{a+\sqrt{n}}{c}; \alpha \in Q^{***}(\sqrt{n}) : c \equiv 6(mod9)\}$$

and

$$B = \{\frac{a+\sqrt{n}}{c}; \alpha \in Q^{***}(\sqrt{n}) : c \equiv 3(mod9)\}.$$

Proof. Let $\frac{a+\sqrt{n}}{c} \in Q^{***}(\sqrt{n})$ and $n \equiv 3(mod9)$. Thus by Lemma 2.1 we have $a \equiv 0(mod3)$. Then $a^2 \equiv 0(mod9)$. Hence $bc \equiv -3(mod9)$ as $bc \equiv a^2 - n(mod9)$, so $bc \equiv 6(mod9)$. Let $\frac{a+\sqrt{n}}{c} \in A$ and $b \equiv 1(mod3)$ implies that $b \equiv 1, 4$ or $7(mod9)$. Thus we are left with $c \equiv 6(mod9)$ only. For $\frac{a+\sqrt{n}}{c} \in B$ and $b \equiv 2(mod3)$ implies that $b \equiv 2, 5$ or $8(mod9)$. Thus we have $c \equiv 3(mod9)$. Therefore, for the set A, $c \equiv 6(mod9)$ and for the set B, $c \equiv 3(mod9)$. This completes the proof. □

Corollary 3.2. *Let n be a non-square positive integer such that $n \equiv 6(mod9)$. Then, the sets A and B of Theorem 3.3 becomes*

$$A = \{\frac{a+\sqrt{n}}{c}; \alpha \in Q^{***}(\sqrt{n}) : c \equiv 3(mod9)\}$$

and

$$B = \{\frac{a+\sqrt{n}}{c}; \alpha \in Q^{***}(\sqrt{n}) : c \equiv 6(mod9)\}.$$

Proof. Proof is straightforward as done in Corollary 3.1. □

Lemma 3.1. *Let*

$$M = \langle x, y : x^2 = y^6 = 1 \rangle$$

and $M' = \langle u, v \rangle$, then prove that $\langle M', x \rangle = M$.

Proof. Since $xy \in M'$, then $xy \in \langle M', x \rangle$. Also $xxy = y \in \langle M', x \rangle$. Therefore, the generators x and y of M are in $\langle M', x \rangle$.

Thus

$$M \subseteq \langle M', x \rangle \tag{1}$$

But clearly, the generators of M' are contained in M. Therefore for $x \in M$, we have,

$$\langle M', x \rangle \subseteq M \tag{2}$$

From equations (1) and (2) it is evident that $\langle M', x \rangle = M$. □

Note: By above lemma, we know that $\langle M', x \rangle = M$. Therefore:

$$Q^*(\sqrt{n}) \bigcup \left\{ \frac{-1}{3\alpha} : \alpha \in Q^*(\sqrt{n}) = Q^*(\sqrt{n}) \bigcup x(Q^*(\sqrt{n})) \right\}$$

is invariant under M. Similarly if any subset A of $Q^*(\sqrt{n})$ is invariant under M', then clearly $A \bigcup x(A)$ is invariant under M. That is, A is M'-subset of $Q^*(\sqrt{n})$. Then $A \bigcup x(A)$ is M'-subset of $Q^{'''}(\sqrt{n})$

4. M-Subsets by using linear congruence

In this section we can classify the elements of $Q^*(\sqrt{n})$ with the modulus $s = 2^u\ 3^v$; $u,\ v \geq 1$.

Example 4.1. By taking $s = 2^1 3^1$, we have classified the elements with respect to the modulo 6 by using the system of linear congruences and we exploit the results in modulo 2 and 3. Also, we are concerned with results for $s = 2^u 3^1$, where $u = 2, 3$ in this section. Since, each non-square n can be considered in the modulo s for any value of $s \geq 1$. For example, in this section if we take $s = 3, 4$. That is $n \equiv 0, 1, 2$ or $3(mod4)$ we have $n \equiv 0, 1$ or $2(mod3)$ as well. As each $n \equiv i(mod4)$ and similarly the same $n \equiv j(mod3)$, where $0 \leq i \leq 3$ and $0 \leq j \leq 2$. Thus, by using the method of solving linear congruence, we can obtain solutions of these congruences in the modulo 12.

Example 4.2. The solution of the congruences $n \equiv 0(mod4)$ and$n \equiv 0(mod3)$ in the modulo 12 is $n \equiv 0(mod12)$. Similarly, $n \equiv 0(mod4)$ and $n \equiv 1(mod3)$ implies $n \equiv 4(mod12)$. Also, $n \equiv 0(mod4)$ and $n \equiv 2(mod3)$ leads to $n \equiv 8(mod12)$.

We need the following theorems from number theory:

Theorem 4.1. *[1] Let $m > 1$ be fixed and a, b, c and d be arbitrary integers, then the following properties hold*

i) $a \equiv a(modm)$,

ii) If $a \equiv b(modm)$, then $b \equiv a(modm)$,

iii) If $a \equiv b(modm)$ and $b \equiv c(modm)$, then $a \equiv c(modm)$,

iv) If $a \equiv b(modm)$ and $c \equiv d(modm)$, then $a + c \equiv b + d(modm)$ and $ac \equiv bd(modm)$,

v) If $a \equiv b(modm)$ and $d \mid m, d > 0$, then $a \equiv b(modd)$.

Theorem 4.2. *If a, b, k and m are integers such that $k > 0, m > 0$ and $a \equiv b(modm)$. Then $a^k \equiv b^k(modm)$.*

Now we are in condition to produce our first lemma.

Lemma 4.1. *Let $n \equiv 1(mod12)$ be a non-square positive integer, and*

$$\begin{aligned}
C_1 &= \{\frac{a+\sqrt{n}}{c} \in Q'^{***}(\sqrt{n}) : [a,b,c](mod6) \text{ with } a \equiv 1(mod6)\} \\
C_2 &= \{\frac{a+\sqrt{n}}{c} \in Q'^{***}(\sqrt{n}) : [a,b,c](mod6) \text{ with } a \equiv 5(mod6)\} \\
C_3 &= \{\frac{a+\sqrt{n}}{c} \in Q'(\sqrt{n}) : [a,b,c](mod6) \text{ with } c \equiv 2(mod6)\} \\
C_4 &= \{\frac{a+\sqrt{n}}{c} \in Q'(\sqrt{n}) : [a,b,c](mod6) \text{ with } c \equiv 4(mod6)\} \\
C_5 &= \{\frac{a+\sqrt{n}}{c} \in Q^{***}(\sqrt{n}) \setminus Q'^{***}(\sqrt{n}) : [a,b,c](mod6) \text{ with } a \equiv 1,6(mod6)\} \\
C_6 &= \{\frac{a+\sqrt{n}}{c} \in Q^{***}(\sqrt{n}) \setminus Q'^{***}(\sqrt{n}) : [a,b,c](mod6) \text{ with } a \equiv 2,5(mod6)\} \\
C_7 &= \{\frac{a+\sqrt{n}}{c} \in Q^{*}(\sqrt{n}) : [a,b,c](mod6) \text{ with } c \equiv 1,4(mod6)\} \\
C_8 &= \{\frac{a+\sqrt{n}}{c} \in Q^{*}(\sqrt{n}) : [a,b,c](mod6) \text{ with } c \equiv 2,5(mod6)\}
\end{aligned}$$

are M'-subsets.

Proof. We know that the elements of $Q^*(\sqrt{n})$ of the forms $[a,b,c](mod2)$ are exactly 4 for $n \equiv 1(mod4)$ and for $n \equiv 1(mod3)$ the elements of $Q^*(\sqrt{n})$ are exactly 12 of the forms $[a,b,c](mod3)$. Therefore, if $n \equiv 1(mod12)$ then the elements of $Q^*(\sqrt{n})$ of the forms $[a,b,c](mod6)$ are 48 in number.

It is well known that if $a^2 - n \equiv 1(mod3)$ has k_1 solutions and $a^2 - n \equiv 1(mod2)$ has k_2 solutions, then $a^2 - n \equiv 1(mod2.3) \equiv 1(mod6)$ has $k_1\ k_2$ solutions by Theorem 4.2.

Let $\frac{a+\sqrt{n}}{c} \in C_1$, since $n \equiv 1(mod12)$ implies that $n \equiv 1(mod6)$ by Theorem 4.1(v).

Given $a \equiv 1(mod6)$ implies $a^2 \equiv 1(mod6)$and also $c \equiv 0(mod6)$ since $\frac{a+\sqrt{n}}{c} \in Q'^{***}(\sqrt{n})$. Thus $bc \equiv a^2 - n(mod6)$ gives us $bc \equiv 0(mod6)$. Also, $c \equiv 0(mod6)$ forces that $b \equiv 0, 2or4(mod6)$ as $[a, b, c](mod6)$ is basically of the form $[1, 0, 0](mod2)$. Therefore, the elements of C_1 are of the forms $[1, 0, 0]$,$[1, 2, 0]$ and $[1, 4, 0](mod6)$ only.

Let $\frac{a+\sqrt{n}}{c} \in C_2$. Given $a \equiv 5(mod6)$ implies $a^2 \equiv 1(mod6)$. Thus $bc \equiv a^2 - n(mod6)$ gives $bc \equiv 0(mod6)$. Also, $c \equiv 0(mod6)$ forces that $b \equiv 0, 2$ or $4(mod6)$ as $[a, b, c](mod6)$ is basically of the form $[1, 0, 0](mod2)$. Therefore, the elements of C_2 are of the forms $[5, 0, 0]$, $[5, 2, 0]$ and $[5, 4, 0](mod6)$.

Since

$$C_1 = \left\{ \frac{a+\sqrt{n}}{c} \in Q'^{***}(\sqrt{n}) : [a, b, c](mod6) \text{ with } c \equiv 0(mod6) \text{ and } a \equiv 1(mod6) \right\},$$

here $a \equiv 1(mod6)$ implies that $a \equiv 1(mod3)$, also $c \equiv 0(mod3)$ since $c \equiv 0(mod6)$.

Therefore we have

$$C_1 = \{\frac{a+\sqrt{n}}{c} \in Q'^{***}(\sqrt{n}) : [a, b, c](mod6) \text{ with } a \equiv 1(mod6)\}$$

is an M'-subset. Similarly, it can be checked for C_2. In this way one can prove that C_3, C_4, C_5, C_6, C_7 and C_7 are M'-subsets. □

Also we have the following important lemmas by using the method of solving linear congruences in modulo12.

Lemma 4.2. *Let $n \equiv 5(mod12)$ be a non-square positive integer, and*

$$\begin{aligned}
D_1 &= \{\frac{a+\sqrt{n}}{c} \in Q'(\sqrt{n}) : [a, b, c](mod6) \text{ with } c \equiv 2(mod6)\} \\
D_2 &= \{\frac{a+\sqrt{n}}{c} \in Q'(\sqrt{n}) : [a, b, c](mod6) \text{ with } c \equiv 4(mod6)\} \\
D_3 &= \{\frac{a+\sqrt{n}}{c} \in Q^*(\sqrt{n}) \setminus Q'(\sqrt{n}) : [a, b, c](mod6) \text{ with } c \equiv 1 \text{ or } 4(mod6)\} \\
D_4 &= \{\frac{a+\sqrt{n}}{c} \in Q^*(\sqrt{n}) \setminus Q'(\sqrt{n}) : [a, b, c](mod6) \text{ with } c \equiv 2 \text{ or } 5(mod6)\}
\end{aligned}$$

are M'-subsets.

Lemma 4.3. *Let $n \equiv 9(mod12)$ be a non-square positive integer, and*

$$E_1 = \{\frac{a+\sqrt{n}}{c} \in Q'^{***}(\sqrt{n}) : [a,b,c](mod6) \ with \ a \equiv 2(mod6)\}$$
$$E_2 = \{\frac{a+\sqrt{n}}{c} \in Q'^{***}(\sqrt{n}) : [a,b,c](mod6) \ with \ a \equiv 4(mod6)\}$$
$$E_3 = \{\frac{a+\sqrt{n}}{c} \in Q'(\sqrt{n}) : [a,b,c](mod6) \ with \ c \equiv 2(mod6)\}$$
$$E_4 = \{\frac{a+\sqrt{n}}{c} \in Q'(\sqrt{n}) : [a,b,c](mod6) \ with \ c \equiv 4(mod6)\}$$
$$E_5 = \{\frac{a+\sqrt{n}}{c} \in Q^{***}(\sqrt{n}) \setminus Q'^{***}(\sqrt{n}) : [a,b,c](mod6) \ with \ b \equiv 1 \ or \ 4(mod6)\}$$
$$E_6 = \{\frac{a+\sqrt{n}}{c} \in Q^{***}(\sqrt{n}) \setminus Q'^{***}(\sqrt{n}) : [a,b,c](mod6) \ with \ b \equiv 2 \ or \ 5(mod6)\}$$
$$E_7 = \{\frac{a+\sqrt{n}}{c} \in Q^{*}(\sqrt{n}) \setminus Q'(\sqrt{n}) : [a,b,c](mod6) \ with \ c \equiv 1 \ or \ 4(mod6)\}$$
$$E_8 = \{\frac{a+\sqrt{n}}{c} \in Q^{*}(\sqrt{n}) \setminus Q'(\sqrt{n}) : [a,b,c](mod6) \ with \ c \equiv 2 \ or \ 5(mod6)\},$$

are M'-subsets.

Proof of these two lemmas is analogous to the proof of Lemma 4.1.

Conclusion

From the last three lemmas we get the following immediate consequences. There are two M'-subsets for $n \equiv 0(mod4)$ given below:

$$\begin{aligned} A =& \{\alpha \in Q^*(\sqrt{n}) : \frac{a+\sqrt{n}}{c} \text{is of forms} \\ & [0,0,1],[0,1,0],[1,1,1],[2,0,1],[2,1,0] \text{ or } [3,1,1]\} \\ B =& \{\alpha \in Q^*(\sqrt{n}) : \frac{a+\sqrt{n}}{c} \text{is of forms} \\ & [0,0,3],[0,3,0],[1,3,3],[2,0,3],[2,3,0] \text{ or } [3,3,3]\} \end{aligned}$$

Also, we combine $n \equiv 0, 1,$ or $2(mod3)$ with the $n \equiv 0(mod4)$. Thus we obtain eight M'-subsets for $n \equiv 0(mod12)$, $n \equiv 8(mod12)$ and four M'-subsets when $n \equiv 4(mod12)$. We have two M'-subsets for $n \equiv 3(mod4)$ given as:

$$\begin{aligned} A =& \{\alpha \in Q^*(\sqrt{n}) : \frac{a+\sqrt{n}}{c} \text{is of forms} \\ & [0,1,1],[1,1,2],[1,2,1],[2,1,1],[3,1,2] \text{ or } [3,2,1]\} \\ B =& \{\alpha \in Q^*(\sqrt{n}) : \frac{a+\sqrt{n}}{c} \text{is of forms} \\ & [0,3,3],[1,2,3],[1,3,2],[2,3,3],[3,2,3] \text{ or } [3,3,2]\} \end{aligned}$$

Then, after combining $n \equiv 0, 1,$ or $2(mod3)$ with the $n \equiv 3(mod4)$, we have eight M'-subsets if $n \equiv 3(mod12)$, $n \equiv 7(mod12)$ and four M'-subsets if $n \equiv 11(mod12)$.

When $n \equiv 3(mod4)$ we have two M'-subsets for each $n \equiv 2(mod8)$ and $n \equiv 6(mod8)$. Also, we combine $n \equiv 0, 1$ or $2(mod3)$ with these two relations.

Thus we get classes in the modulo 24. Therefore, M'-subsets for $n \equiv 2, 6$ or $10(mod12)$ can be calculated by the above technique.

Acknowledgements

The authors wish to thank the referees for their valuable suggestions which improved the paper.

References

[1] Burton, D. M., Elementary Number Theory. Tata McGraw-Hill publishing company Limited. 2007.

[2] Afzal, F., Afzal, Q., Malik, M. A., A Classification of the Real Quadratic Irrational Numbers $\frac{a+\sqrt{n}}{c}$ of $Q^*(\sqrt{n})$ w.r.t, Modulo 3^{rd}. International Mathematical Forum, Vol. 7, No. 39(2012), 1915-1924.

[3] Higman, G., Mushtaq, Q., Coset Diagrams and Relations for PSL $(2, Z)$. Arab Gulf J. Sc, Vol. 1 No.1(1983), $159 - 164$.

[4] Kouser, I., Husnine, S. M., Majeed, A., A Classification of the elements of $Q^*(\sqrt{p})$ and a partition of $Q^*(\sqrt{p})$ under the Modular Group action. PUJM, Vol. 31 (1998), 103-118.

[5] Ashiq, M., Action of a Two Generated Group on Real Quadratic Fields. Southeast Asian Bulletin of Mathematics, Vol.30(2006), $399 - 404$.

[6] Ashiq, M., Mushtaq, Q., Action of a Subgroup of Two Generated Group on an Imaginary Quadratic Fields. Quasigroups and Related Systems, Vol. 14(2006), $133 - 146$.

[7] Malik, M. A., Husnine, S. M., Majeed, A., Modular Group Action on Certain Quadratic Fields. PUJM, Vol. 28(1995), $47 - 68$.

[8] Malik, M. A., Husnine, S. M., Majeed, A., On Invariant subsets of certain Quadratic Fields under Modular Group Action. PUJM, Vol. 29(1996), $20 - 26$.

[9] Malik, M. A., Groups Action on Fields, D. Phil. Thesis. University of the Punjab, Lahore, Pakistan, 2002.

[10] Malik, M. A., Husnine, S. M., Majeed, A., Action of a group $M = \langle x, y : x^2 = y^6 = 1\rangle$ on Certain Real Quadratic Fields. PUJM, Vol. 36(2004), $71 - 88$.

[11] Malik, M. A., Husnine, S. M., Majeed, A., Action of a group $M = \langle x, y : x^2 = y^6 = 1\rangle$ on Certain Real Quadratic Fields-II. PUJM, Vol. 44(2012), $1 - 7$.

[12] Malik, M. A., Husnine, S. M., Majeed, Properties of Real Quadratic irrational numbers under the action of the group $H = \langle x, y : x^2 = y^4 = 1\rangle$. Studia Scientiartum Mathematicarum Hungarica, Vol. 42 No.4 (2005), $371 - 386$.

[13] Malik, M. A., Mehmood, K. M., Some Invariant subsets of $Q^*(\sqrt{n})$ under the action of PSL $(2, Z)$. International Mathematical Forum, Vol. 6, No. 32(2011), $1557 - 1565$.

[14] Malik, M. A., Zafar, M. A., Real Quadratic Irrational Numbers and Modular group Action. Southeast Asian bulletin of Mathematics, Vol.35 No.3(2011), $439 - 445$.

[15] Aslam,M., Intransitive action of $\langle y, t; y^4 = t^4 = 1\rangle$ acting on $Q(\sqrt{n})$. PUJM, Vol. 35(2002), $1 - 6$.

[16] Aslam, M., Mushtaq, Q., Masood, T., Ashiq, M., Real Quadratic irrational numbers and the group $\langle x, y; x^2 = y^6 = 1\rangle$. Southeast Asian Bulletin of Mathematics, Vol.27(2003), $409 - 415$.

[17] Mushtaq, Q., Some Remarks on Coset Diagrams for the Modular Group. Math. Chronical, Vol. 16(1987), $69 - 77$.

[18] Mushtaq, Q., Modular Group Acting on Real Quadratic Fields. Bull Austral Math Soc, Vol. 37(1988), $303 - 309$.

[19] Mushtaq, Q., The Extended Modular Group Acting on the projective line over a Galois Field. Indian J. Pure App. Math, Vol. 20 No. 8(1989), $755 - 760$.

[20] Mushtaq, Q., Shaheen,F., Some Special Circuits in Coset Diagrams. Math. Japonica, Vol 37, No.1(1992), $149 - 158$.

[21] Mushtaq, Q., Aslam, M., Group Generated by two elements of orders 2 and 4 acting on real quadratic fields. Acta Mathematica Sinica. New Series, Vol. 9, No.1(1993), $221 - 224$.

Received by the editors March 26, 2012