INVARIANT SUBSETS OF $PLQ(\sqrt{m})$ UNDER THE ACTION OF $M = \langle x, y : x^2 = y^6 = 1 \rangle$

M. Aslam Malik and Nosheen Goshi

Department of Mathematics, University of the Punjab, Quaid-e-Azam Campus, Lahore-54590, Pakistan.
Corresponding Author: malikpu@yahoo.com

Let $n = k^2 m$. Then $Q^*(\sqrt{n}) = \{\frac{a+\sqrt{n}}{c} : a, c, \frac{a^2-n}{c} \in Z, (a, \frac{a^2-n}{c}, c) = 1\}$ is a G-subset of $Q(\sqrt{m}) \setminus Q$ where $G = \langle x, y : x^2 = y^3 = 1 \rangle$. In this paper we find proper M-subsets of $Q^{***}(\sqrt{n}) = \{\frac{a+\sqrt{n}}{c} \in Q^*(\sqrt{n}) : c \equiv 0 (mod\ 3)\}$ *or* $Q^{*\sim}(\sqrt{n}) = Q^*(\sqrt{\frac{n}{9}}) \setminus Q^{***}(\sqrt{\frac{n}{9}})) \cup Q^{***}(\sqrt{n})$ according as $n \not\equiv 0 (mod\ 9)$ or $n \equiv 0 (mod\ 9)$ and $Q^{*\sim}(\sqrt{9n}) = (Q^*(\sqrt{n}) \setminus Q^{***}(\sqrt{n})) \cup Q^{***}(\sqrt{9n})$ for all n which are invariant subsets of $Q(\sqrt{m}) \setminus Q$ under the action of $M = \langle x, y : x^2 = y^6 = 1 \rangle$. Specifically we show that $o_M^{*\sim}(9p) = o_G(9p)$ for all prime p, where $o_M^{*\sim}(9p)$ denotes the number of M-orbits of $Q^{*\sim}(\sqrt{9p})$ and $o_G(9p)$ denotes the number of G-orbits of $Q^*(\sqrt{9p})$. Also we prove that $o_M^{***}(p) = o_G(p)$ if $p \equiv 1 (mod\ 3)$ where $o_M^{***}(p)$ denotes the number of M-orbits of $Q^{***}(\sqrt{p})$.

AMS Mathematics subject classification (2000): 05C25, 11E04, 20G15
Keywords: Quadratic residue; Möbius Group; Linear-fractional Möbius transformations; M-orbit.

INTRODUCTION AND PRELIMINARIES

An extension of degree 2 of the field of rational numbers Q is called the real quadratic field $Q(\sqrt{m})$, where $m > 0$ is square free integer. Since $PLQ(\sqrt{m}) = Q(\sqrt{m}) \cup \{\infty\} = (Q(\sqrt{m}) \setminus Q) \cup (Q \cup \{\infty\})$.

$Q^*(\sqrt{n}) = \{\frac{a+\sqrt{n}}{c} : a, c, \frac{a^2-n}{c} \in Z, (a, \frac{a^2-n}{c}, c) = 1\}$ is a G-subset of $Q(\sqrt{m}) \setminus Q$ where $n = k^2 m$. Since $Q^*(\sqrt{n})$ and $Q^*(\sqrt{n'})$ are disjoint if and only if n, n' are distinct integers, so $Q(\sqrt{m}) \setminus Q = \bigcup_{k \in N} Q^*(\sqrt{k^2 m})$ is disjoint union. It was proved in 1988 by Mushtaq and Aslam, that the action of M on $Q \cup \{\infty\}$ is transitive whereas the action of M on $Q(\sqrt{m}) \setminus Q$ is intransitive was proved in 2004, by Malik *et al* ., by proving that $Q''(\sqrt{n}) = \{\frac{\alpha}{t} : \alpha \in Q^*(\sqrt{n}); t = 1,3\} = Q^*(\sqrt{n}) \cup \frac{1}{3} Q^*(\sqrt{n})$ is an M-subset of $Q(\sqrt{m}) \setminus Q = \bigcup_{k \in N} Q''(\sqrt{k^2 m})$. The group $G = \langle x, y : x^2 = y^3 = 1 \rangle$ where $x(\alpha) = \frac{-1}{\alpha}$ and $y(\alpha) = \frac{\alpha - 1}{\alpha}$ are the linear fractional transformations, is the Modular group. The group $M = \langle x, y : x^2 = y^6 = 1 \rangle$ where $x(\alpha) = \frac{-1}{3\alpha}$ and $y(\alpha) = \frac{-1}{3(\alpha+1)}$ are the Möbius transformations, is the Möbius group. Since $Q''(\sqrt{n}) \cap Q''(\sqrt{9n}) = (Q^*(\sqrt{n}) \setminus Q^{***}(\sqrt{n})) \cup Q^{***}(\sqrt{9n})$ for each non square n, so $Q(\sqrt{m}) \setminus Q = \bigcup_{k \in N} Q''(\sqrt{k^2 m})$ is not disjoint union. However this reduces the study of action of M on $Q(\sqrt{m}) \setminus Q$ to the study of action of M on $Q''(\sqrt{n})$.

For brevity we denote $(Q^*(\sqrt{n}) \setminus Q^{***}(\sqrt{n})) \cup Q^{***}(\sqrt{9n})$ by $Q^{*\sim}(\sqrt{9n})$ for all non square n.

Then:

$$Q''(\sqrt{n}) = \begin{cases} Q^{***}(\sqrt{n}) \cup Q^{*\sim}(\sqrt{9n}) & if\ n \equiv 1,3,4,6\ or\ 7 (mod\ 9) \\ Q^{*\sim}(\sqrt{n}) \cup Q^{*\sim}(\sqrt{9n}) & if\ n \equiv 0 (mod\ 9) \\ Q^{*\sim}(\sqrt{9n}) & if\ n \equiv 2,5\ or\ 8 (mod\ 9) \end{cases}$$

Hence this further reduces the study of action of M on $Q''(\sqrt{n})$ to the study of the action of M on $Q^{***}(\sqrt{n})$ or $Q^{*\sim}(\sqrt{n})$ according as $n \not\equiv 0(mod\ 9)$ or $n \equiv 0(mod\ 9)$ and $Q^{*\sim}(\sqrt{9n})$ for all non-square n. An element $\frac{a+\sqrt{n}}{c} \in Q^*(\sqrt{n})$ is called ambiguous number if and only if $a^2 < n$ and $Q_1^*(\sqrt{n})$, $Q_1^{***}(\sqrt{n})$, $Q_1^{*\sim}(\sqrt{n})$, $Q_1^{''}(\sqrt{n})$ stands for the set of ambiguous numbers of $Q^*(\sqrt{n})$, $Q^{***}(\sqrt{n})$, $Q^{*\sim}(\sqrt{n})$, $Q^{''}(\sqrt{n})$ respectively.

In 1978, G. Higman used the idea of coset diagram (generalization of Cayley graphs) to study the action of such finitely generated infinite groups on infinite fields for the first time. In 1995 (Malik *et al* .), the cardinality of $Q_1^*(\sqrt{n}) = \{\frac{a+\sqrt{n}}{c} \in Q^*(\sqrt{n}) : a^2 < n\}$ was determined. In 1988, by Mushtaq and Aslam, it was proved that the ambiguous numbers in the coset diagram under the action of Möbius group form a single closed path and it is the only closed path contained in each orbit, α^M, where $\alpha \in Q(\sqrt{m}) \setminus Q$. Both these results urge one to think how many such paths exist under the action of M on $Q^{''}(\sqrt{n})$.

It is quite appealing to relate the group action on quadratic field to new and fascinating multi-front of algebraic number theory. It is easy to see that the set $Q^*(\sqrt{n})$ is the set of all roots of the primitive second degree equations $ct^2 + 2at + b = 0$ with reduced discriminant $\Delta = a^2 - bc = n$. If α is the root of the equation $ct^2 + 2at + b = 0$, then $x(\alpha)$ and $y(\alpha)$ are the roots of the second degree equations $3bt^2 + 2at + \frac{c}{3} = 0$ and $3(2a+b+c)t^2 + 2(a+c)t + \frac{c}{3} = 0$ respectively. It is worth noticing that all these three equations admit the same reduced discriminant, Δ. This shows that $Q''(\sqrt{n})$ is an M-subset of $Q(\sqrt{m}) \setminus Q$ and hence for each $n \not\equiv 0(mod\ 9)$, $Q^{***}(\sqrt{n}) = \{\frac{a+\sqrt{n}}{c} \in Q^*(\sqrt{n}) : c \equiv 0(mod\ 3)\}$ is an M-subset of $Q''(\sqrt{n})$. If α and its algebraic conjugate $\overline{\alpha}$ have opposite signs then α is called ambiguous number.

The action of G on $Q^*(\sqrt{n})$ was discussed by (Malik *et al* ., 2000, 2004), and it was proved that G acts on $Q^*(\sqrt{2})$ transitively whereas the action of G on $Q^*(\sqrt{n}), n \neq 2$ is intransitive. The exact number of ambiguous numbers in $Q^*(\sqrt{n})$ for all non-square n as a function of n was determined by (Malik *et al* ., 2004). The M-subsets of $Q'''(\sqrt{n})$ were explored in (Malik *et al* ., 2004, 2012) by using coset diagram. Closed paths in the coset diagrams for a subgroup of M acting on $Q(\sqrt{m})$ were studied by Aslam and Mushtaq, 2004. The orbits of $Q^*(\sqrt{n})$ under the action of G were discussed by (Kouser *et al* ., 2000, Malik and Aneesa 2011, 2012) and it has been investigated that the number $o_G(p)$, the number of G-orbits of $Q^*(\sqrt{p})$, is even. It is quite captivating to explore the transitive M-subsets of $Q''(\sqrt{n})$ and to determine the number $o_M(n)$ of M-orbits of $Q''(\sqrt{n})$ in terms of $o_G(n)$

Throughout this paper G and M stands for Modular and Möbius group respectively, n for non-square positive, α for $\frac{a+\sqrt{n}}{c}$, $(\bullet/\bullet)$ for Legendre symbol, $o_M^{*\sim}(n)$ when $n \equiv 0(mod\ 9)$ (respectively $o_M^{***}(n)$ when $n \not\equiv 0(mod\ 9)$) denotes the number of M-orbits of $Q^{*:}(\sqrt{n})$ (respectively $Q^{***}(\sqrt{n})$). $o_M^{*\sim}(9n)$ denote the number of M-orbits of $Q^{*\sim}(\sqrt{9n})$. In what follows throughout that p is an odd prime, unless otherwise mentioned.

In Section 2 we study the action of M on $Q'''(\sqrt{n})$ and determine cardinalities of some M-subsets of $Q''(\sqrt{n})$. We prove that

$$o_M^{*\sim}(9p) = o_G(9p)$$

and find $o_M(p)$ in terms of $o_G(p)$.

Section 3 is concerned with the M-orbits of $Q^{*\sim}(\sqrt{9p})$ when $p \equiv 1(mod\ 4)$. In particular we have been able to prove that $Q^{*\sim}(\sqrt{9p})$ splits into

atleast four M-orbits when $p \equiv 1(mod\ 4)$. In Section 4, we further find some more M-orbits when $|(\sqrt{p})^M|_{amb} + |(\frac{\sqrt{p}}{-1})^M|_{amb} + |(\frac{1+\sqrt{p}}{2})^M|_{amb} + |(\frac{-1+\sqrt{p}}{-2})^M|_{amb} < |Q_1^{*\sim}(\sqrt{9p})|$ and prove that $(\alpha)^M \cap (\overline{\alpha})^M = \varnothing$ and $(\alpha)^M \cap (-\alpha)^M = \varnothing$ for all $\alpha \in Q^{*\sim}(\sqrt{9n}) \setminus ((\sqrt{n})^M \cup (\frac{\sqrt{n}}{-1})^M \cup (\frac{1+\sqrt{n}}{2})^M \cup (\frac{-1+\sqrt{n}}{-2})^M)$.

To accomplish our work we enlist several already proved lemmas that will be used in the subsequent work.

Lemma 1.1 (Malik *et al*., 1995) Let m be a square-free positive integer. Then:

$$|Q_1^*(\sqrt{m})| = \tau^*(m) = 2\tau(m) + 4\sum_{a=1}^{\lfloor\sqrt{m}\rfloor}\tau(m-a^2)$$

Lemma 1.2 (Malik *et al*., 2000) Let $p \equiv 1(mod\ 4)$ such that $p = a^2 + c^2$. Then there are exactly eight numbers

$$\frac{a+\sqrt{p}}{\pm c}, \frac{-a+\sqrt{p}}{\pm c}, \frac{c+\sqrt{p}}{\pm a}, \frac{-c+\sqrt{p}}{\pm a}\ of\ Q_1^*(\sqrt{p})$$

which are mapped onto their conjugates under x.

Lemma 1.3 (Malik *et al*., 2000) Let $p \equiv 1(mod\ 4)$. Then $Q^*(\sqrt{p})$ splits into at least two G-orbits, namely, $(\sqrt{p})^G$ and $(\frac{1+\sqrt{p}}{2})^G$ under the action of G.

Lemma 1.4 (Malik and Aneesa, 2012) Let $p \equiv 1(mod\ 4)$. Then: $|(\sqrt{p})^G|_{amb} = 8\lfloor\sqrt{p}\rfloor$ and $|(\frac{1+\sqrt{p}}{2})^G|_{amb} = 4(\lfloor\sqrt{p}\rfloor + 1)$ where $p-1$ is a perfect square.

$|(\sqrt{p})^G|_{amb} = 4(3\lfloor\sqrt{p}\rfloor + 1)$ and $|(\frac{1+\sqrt{p}}{2})^G|_{amb} = 4\lfloor\sqrt{p}\rfloor$ where $p-4$ is a perfect square.

Lemma 1.5 (Malik *et al*., 2004) Let $\alpha = \frac{a+\sqrt{n}}{c} \in Q^*(\sqrt{n})\ and\ b = \frac{a^2-n}{c}$. Then:

1. $\frac{\alpha}{3} \in Q^{***}(\sqrt{n}) \Leftrightarrow 3 \mid b.$
2. $\frac{\alpha}{3} \in Q^{***}(\sqrt{9n}) \Leftrightarrow 3\ \text{does not divide}\ b$.

Lemma 1.6 (Malik *et al*., 2012) Let $X_1 = \{\alpha : \alpha \in Q^*(\sqrt{n})\ with\ c\ or\ b \equiv 1(mod\ 3)\}$ and $X_3 = \{\alpha : \alpha \in Q^*(\sqrt{n})\ with\ c\ or\ b \equiv 2(mod\ 3)\}$. Then $X_1 \cup x(X_1)$ and $X_3 \cup x(X_3)$ are M-subsets of $Q^{*\sim}(\sqrt{9n})$.

Lemma 1.7 (Malik *et al*., 2012) ~

$$Q''(\sqrt{n}) \setminus Q^*(\sqrt{n}) = \begin{cases} Q^{***}(\sqrt{9n}) & if\ n \not\equiv 0(mod 9) \\ Q^{***}(\sqrt{9n}) \cup (Q^*(\sqrt{\frac{n}{9}}) \setminus Q^{***}(\sqrt{\frac{n}{9}})) & if\ n \equiv 0(mod 9) \end{cases}$$

Lemma 1.8 (Malik *et al*., 2012) Let $n \equiv 0(mod\ 9)$ and $\alpha \in Q^*(\sqrt{n})$. Then:

1. If *3* does not divide *a* then $\frac{\alpha}{3}$ belongs to $Q^{***}(\sqrt{9n})$
2. If $3 \mid a$ then $\frac{\alpha}{3}$ belongs to $Q^*(\sqrt{\frac{n}{9}}) \setminus Q^{***}(\sqrt{\frac{n}{9}})$ or $Q^{***}(\sqrt{9n})$ according as $\alpha \in Q^*(\sqrt{n}) \setminus Q^{***}(\sqrt{n})$ or $Q^{***}(\sqrt{n})$.

Lemma 1.9 (Malik *et al*., 1995) Let n be square free positive integer. Then: $|Q_1^{***}(\sqrt{n})| = 2\tau'''(n) + 4\sum_{a=1}^{\lfloor\sqrt{n}\rfloor}\tau'''(n-a^2)$ where $\tau'''(u)$ denotes those divisors of u, which are divisible by 3.

Lemma 1.10 (Malik *et al*., 2004) Let $\alpha \in Q''(\sqrt{n})$. Then $\alpha^M = (\overline{\alpha})^M$ if and only if there exists an element β in α^M such that $x(\beta) = \overline{\beta}$

2 M-subsets of $Q'''(\sqrt{k^2 m})$

We start this section with the following definition.

Definition 2.1 By a circuit, we shall mean closed path of edges and hexagons in the coset diagram for M-orbit $\alpha^M\ where\ \alpha \in Q^*(\sqrt{n})$.

If $n_1, n_2, n_3, n_4, ..., n_k$ is a sequence of positive integers

and

$$i_j = 0,1,2,3,4, i_l \neq i_{l+1}\ (l = 1,2,...,k-1), i_1 \neq i_k \qquad (1)$$

Then by a circuit of the type $(n_{1i_1}, n_{2i_2}, n_{3i_3}, n_{4i_4}, ..., n_{ki_k})$ we shall mean the circuit (counter clockwise) in which $n_j, j = 1,2,3,...,k$ hexagons have i_j vertices outside the circuit.

Remarks 2.2 1. Since it is immaterial with which ambiguous number of α^H the circuit begins, we can express type (1) by any of the following k-equivalent forms

$$(n_{1i_1}, n_{2i_2}, ..., n_{ki_k}) = (n_{2i_2}, n_{3i_3}, ..., n_{ki_k}, n_{1i_1})$$

$$= ...(n_{ki_k}, n_{1i_1}, ..., n_{k-1i_{k-1}})$$

2. The type $(n_{1i_1}, n_{2i_2}, n_{3i_3}, n_{4i_4}, ..., n_{ki_k})$ can be described by the equations (1) or more briefly by

$$i_j = 0,1,2,3,4, i_t \neq i_{t+1(mod\ k)} \quad (2)$$

3. This circuit induces an element $g = (xy^{i_k+1})^{n_k} ... (xy^{i_2+1})^{n_2} (xy^{i_1+1})^{n_1}$ of H and fixes a particular vertex of a hexagon lying on the circuit and hence the ambiguous length of this circuit is given by $2(n_1 + n_2 + n_3 + ... + n_k)$

4. All of the $2(n_1 + n_2 + ... + n_k)$ numbers lies in the same orbit and hence each of them has the same type.

For example, by the circuit of the type $(2_0, 1_1, 3_4, 1_3, 2_2, 6_0)$ we mean the circuit induces an element $g = (xy)^6 (xy^3)^2 (xy^4)(xy^5)^3 (xy^2)(xy)^2$ of M which fixes some vertex k and the ambiguous length of this circuit will be $2(2+1+3+1+2+6)$.

Next in this section we are concerned with the ambiguous cardinalities of M-subsets of $Q'''(\sqrt{n})$. In the following lemma we find the condition for the sets $(Q^*(\sqrt{n}) \setminus Q^{***}(\sqrt{n})$ and $Q^*(\sqrt{n})$ to be equivalent to $Q^{***}(\sqrt{9n})$.

Lemma 2.3

$$Q^{***}(\sqrt{9n}) \text{ is equivalent to } \begin{cases} Q^*(\sqrt{n}) & \text{if } n \equiv 2(mod\ 3) \\ Q^*(\sqrt{n}) \setminus Q^{***}(\sqrt{n}) & \text{if } n \not\equiv 2(mod\ 3) \end{cases}$$

Proof: The proof follows by the mapping

$$x : Q^{***}(\sqrt{9n}) \to \begin{cases} Q^*(\sqrt{n}) & \text{if } n \equiv 2(mod\ 3) \\ Q^*(\sqrt{n}) \setminus Q^{***}(\sqrt{n}) & \text{if } n \not\equiv 2(mod\ 3) \end{cases}$$

defined by $x(\alpha) = \frac{-1}{3\alpha}$. Clearly the mapping is a bijection. □

The following corollary is an immediate consequence of Lemma 2.3.

Corollary 2.4

$$|Q_1^{***}(\sqrt{9n})| = \begin{cases} |Q_1^*(\sqrt{n})| & \text{if } n \equiv 2(mod\ 3) \\ |Q_1^*(\sqrt{n}) \setminus Q_1^{***}(\sqrt{n})| & \text{if } n \not\equiv 2(mod\ 3) \end{cases}$$

The following lemmas give us cardinality of $Q_1^{*\sim}(\sqrt{9n})$.□

Lemmas 2.5

1.

$$|Q_1^{*\sim}(\sqrt{9n})| = \begin{cases} 2|Q_1^*(\sqrt{n})| & \text{if } n \equiv 2(mod\ 3) \\ 2(|Q_1^*(\sqrt{n})| - |Q_1^{***}(\sqrt{n})|) & \text{if } n \not\equiv 2(mod\ 3) \end{cases}$$

2. $|Q_1^{*\sim}(\sqrt{n})| = 2(|Q_1^{***}(\sqrt{n})|)$ if $n \equiv 0(mod\ 9)$.

Proof: The proof directly follows from the definition of $Q^{*\sim}(\sqrt{9n})$ and Lemma 2.3. □

The following lemmas give us the cardinality of $Q_1'''(\sqrt{n})$.

Lemmas 2.6

$$|Q_1'''(\sqrt{n})| = \begin{cases} |Q_1^{*\sim}(\sqrt{9n})| = 2|Q_1^*(\sqrt{n})| & \text{if } n \equiv 2(mod 3) \\ 2(|Q_1^*(\sqrt{n})|) - |Q_1^{***}(\sqrt{9n})| & \text{if } n \equiv 1,3,4,6 \text{ or } 7(mod 9) \\ |Q_1^{*\sim}(\sqrt{9n})| + |Q_1^{*\sim}(\sqrt{n})| = 2|Q_1^*(\sqrt{n})| & \text{if } n \equiv 0(mod 9) \end{cases}$$

Proof: The proof directly follows from the definition of $Q'''(\sqrt{n})$, Lemmas 2.3 and 2.5. □

3 M-Orbits of $Q'''(\sqrt{p})$ and $Q^{*\sim}(\sqrt{9p})$

Since $p \equiv 1 \text{ or } 2(mod\ 3)$ for each $p \geq 5$ and similarly $p \equiv 1 \text{ or } 3(mod\ 4)$ for each $p > 2$. Thus $p \equiv 1,7,13 \text{ or } 19(mod\ 24)$ according as $p \equiv 1,7,5 \text{ or } 3(mod\ 8)$ and $p \equiv 5,11,17 \text{ or } 23(mod\ 24)$ according as $p \equiv 5,3,1 \text{ or } 7(mod\ 8)$. In Theorem 4.4 (see Malik *et al*., 2000) it has been proved that if $p \equiv 1(mod\ 4)$, then $Q^*(\sqrt{p})$ splits into atleast two G-orbits, namely $(\sqrt{p})^G$ *and* $(\frac{1+\sqrt{p}}{2})^G$. Two M-subsets namely $A \cup x(A)$ *and* $B \cup x(B)$ where

$A = \{\alpha : \alpha \in Q^*(\sqrt{n}) \text{ with } (b/3) \text{ or } (c/3) = 1\}$ and
$B = \{\alpha : \alpha \in Q^*(\sqrt{n}) \text{ with } (b/3) \text{ or } (c/3) = -1\}$ were found by Malik *et al*., 2012. In this section we also determine M -orbits of $Q^{*\sim}(\sqrt{9p})$ and investigate ambiguous lengths of these orbits in terms of p where $p \equiv 1(mod\ 4)$. In the following theorem we discuss the number $o_M(p)$ of M -orbits of $Q''(\sqrt{p})$ in terms of number $o_G(p)$ of G -orbits of $Q^*(\sqrt{p})$ for all p.

Theorem 3.1 If $p > 3$ such that $p \neq 31$. Then: $o_M^{*\sim}(9p) = o_G(9p)$

Proof: If X is any G -orbit of $Q^*(\sqrt{9p})$, then clearly $X \cap Q^{***}(\sqrt{9p}) = \{\alpha \in X : c \equiv 0(mod\ 3)\}$ is not empty and hence $(X \cap Q^{***}(\sqrt{9p})) \cap (Y \cap Q^{***}(\sqrt{9p})) = \varnothing$ whenever X and Y are distinct G -orbits. Then, clearly number of sets of the type $X \cap Q^{***}(\sqrt{9p})$ is $o_G(9p)$. By Lemma 2.3 and Corollary 2.4 we find that the number of M -orbits of $Q^{*\sim}(\sqrt{9p})$, is equal to $o_G(9p)$. This completes the proof.□

In the following remark we give the number of M -orbits of $Q^{***}(\sqrt{p})$ and determine the relationship between the number of G -orbits of $Q^*(\sqrt{p})$ and number of G -orbits of $Q^*(\sqrt{9p})$.

Remark 3.2 It can be easily seen that:

1. $o_M^{*\sim}(p) = o_G(p)$ when $p \equiv 1(mod\ 3)$.
2. $$o_G(9p) = \begin{cases} 2\,o_G(p) & if\ p \not\equiv 11(mod\ 24) \\ 4\,o_G(p) & if\ p \equiv 11(mod\ 24) \end{cases}$$

In the following theorem we give the exact number of M -orbits of $Q^{*\sim}(\sqrt{9p})$ and $Q''(\sqrt{p})$.

Theorem 3.3

1. Let $p \equiv 1(mod\ 3)$ such that $p \neq 31$. Then:
   (a) $o_M^{*\sim}(9p) = 2o_G(p)$
   (b) $o_M(p) = 3o_G(p)$
2. $$o_M(p) = \begin{cases} 2\,o_G(p) & if\ p \equiv 5,17\ or\ 23(mod\ 24) \\ 4\,o_G(p) & if\ p \equiv 11(mod\ 24) \end{cases}$$

Proof: The proof directly follows by using Theorem 3.1 and Remark 3.2.□

Example 3.4 If $p = 31$, then $Q^{*\sim}(\sqrt{9p})$ splits into exactly six M -orbits and $Q^{***}(\sqrt{31})$ splits into two M -orbits whereas $Q^*(\sqrt{31})$ splits into two G -orbits. Also $(\sqrt{31})^G \setminus Q^{***}(\sqrt{31})$ (respectively $(-\sqrt{31})^G \setminus Q^{***}(\sqrt{31})$) splits into three M -orbits namely $(\sqrt{31})^M$, $(\frac{1+\sqrt{31}}{2})^M$ and $(\frac{1+\sqrt{31}}{5})^M$ respectively $(-\sqrt{31})^M$, $(\frac{-1+\sqrt{31}}{-2})^M$ and $(\frac{-1+\sqrt{31}}{-5})^M$). Thus $o_M(31) = 8$. ♦

Example 3.5 Since $o_G(3) = 2$. $Q_1^{***}(\sqrt{3}) = \{\frac{\sqrt{3}}{3}, \frac{\sqrt{3}}{-3}\}$ which map on each other under the action of M and forms a single closed path. Also $Q^{*\sim}(\sqrt{27})$ splits into exactly two distinct M -orbits namely $(\sqrt{3})^M$ and $(\frac{\sqrt{3}}{-1})^M$. Thus $o_M(3) = 3$. ♦

The following lemma will be used in the subsequent work and provides us a base to proceed further.

Lemma 3.6 Let $k \in N$ and for all $\alpha \in Q^*(\sqrt{n})$ Then:

1. $(xy)^k(\alpha) = \alpha + k = (y^5x)^{-k}(\alpha)$
2. $(yx)^k(\alpha) = \dfrac{\alpha}{1-3k\alpha} = (xy^5)^{-k}(\alpha)$

Proof: These results are straightforward and can be verified by Table 1.

Table 1 The action of x, y on $\alpha \in Q''(\sqrt{n})$

α	a	b	c
$xy(\alpha) = \alpha + 1$	$a + c$	$2a + b + c$	c
$(xy)^k(\alpha) = \alpha + k$	$a + kc$	$2ka + b + k^2c$	

$(xy^5)(\alpha)=\frac{\alpha}{3\alpha+1}$	$a+3b\ \ b$	$6a+9b+c$
$(xy^5)^k(\alpha)=\frac{\alpha}{3k\alpha+}$	$a+3kłb$	$6ka+9bk^2+$

In the following theorem we find the ambiguous lengths of M -orbits found in Theorem 3.1 in terms of p.

Theorem 3.7 Let $p\equiv 5(mod\ 12)$ such that $p-1=\lfloor\sqrt{p}\rfloor^2$. Then:

1. $|(\frac{\sqrt{p}}{1})^M|_{amb}=8\sqrt{p-1}=|(\frac{\sqrt{p}}{-1})^M|_{amb}$
2. $|(\frac{1+\sqrt{p}}{2})^M|_{amb}=4(1+\sqrt{p-1})=|(\frac{-1+\sqrt{p}}{-2})^M|_{amb}; p>5$

.

Proof: The proof is analogous to the proof of Theorem 3.1 using the fact given in Remark 3.2.□

Example 3.8

1. By Theorem 3.4, $|(\frac{\sqrt{5}}{1})^M|_{amb}=8=|(\frac{\sqrt{5}}{-1})^M|_{amb}$ and the circuits have the type $(2_0,1_4,2_1,1_4,2_0)$. But Theorem 3.4 doesn't hold for $|(\frac{1+\sqrt{5}}{2})^M|_{amb}=|(\frac{-1+\sqrt{5}}{-2})^M|_{amb}=2$ and circuit have the type $(1_2,1_0)$.
2. By Theorem 3.4, $|(\frac{\sqrt{101}}{1})^M|_{amb}=80=|(\frac{\sqrt{101}}{-1})^M|_{amb}$ and the circuits have the type $(10_0,5_4,1_0,1_3,6_0,1_3,6_4,10_0)$. Also $|(\frac{1+\sqrt{101}}{2})^M|_{amb}=44=|(\frac{-1+\sqrt{101}}{-2})^M|_{amb}$ and the circuit have the type $(4_o,1_2,2_4,1_3,1_5,3_0,1_4,1_3,2_4,1_1,5_0)$.

Remark 3.9 If $p\equiv 5(mod\ 12)$ then the numbers $\frac{\pm\lfloor\sqrt{p}\rfloor+\sqrt{p}}{1}$ and $\frac{\pm\lfloor\sqrt{p}\rfloor+\sqrt{p}}{-1}$ are contained in $(\sqrt{p})^M\ and\ (\frac{\sqrt{p}}{-1})^M$ respectively. Also the numbers $\frac{\pm 1+\sqrt{p}}{\lfloor\sqrt{p}\rfloor}$ are contained in $(\frac{1+\sqrt{p}}{2})^M$ if $\lfloor\sqrt{p}\rfloor\equiv 2(mod\ 3)$ otherwise in $(\frac{-1+\sqrt{p}}{-2})^M$.

Similarly the numbers $\frac{\pm 1+\sqrt{p}}{-\lfloor\sqrt{p}\rfloor}$ are contained in $(\frac{-1+\sqrt{p}}{-2})^M$ if $\lfloor\sqrt{p}\rfloor\equiv 2(mod\ 3)$ otherwise in $(\frac{1+\sqrt{p}}{2})^M$.□

The following theorem is concerned with the type of circuit found in Theorem 3.1.

Theorem 3.10 Let $p\equiv 1(mod\ 12)$ such that $p-1=\lfloor\sqrt{p}\rfloor^2$. Then:

1. The circuits of $(\sqrt{p})^M$ and $(\frac{\sqrt{p}}{-1})^M$ have the type $((\sqrt{p-1})_0,(\frac{2}{3}\sqrt{p-1})_4,(\sqrt{p-1})_0)$ and hence have ambiguous length $\frac{16}{3}(\sqrt{p-1})$.
2. The circuits of $(\frac{1+\sqrt{p}}{2})^M$ and $(\frac{-1+\sqrt{p}}{-2})^M$ have the type $((\lfloor\frac{\sqrt{p-1}}{2}\rfloor)_0,1_2,(\lfloor\frac{\sqrt{p-1}}{3}\rfloor-1)_4,1_2,(\lfloor\frac{\sqrt{p-1}}{2}\rfloor-1)_0)$ and hence have ambiguous length $\frac{8}{3}\sqrt{p-1}$.

Proof: In order to prove second part it is sufficient to find the element $g\in M$ such that $(g)(\frac{1+\sqrt{p}}{2})=\frac{1+\sqrt{p}}{2}$. Using Lemma 3.6 we obtain $(xy)^{\lfloor\frac{\sqrt{p-1}}{2}\rfloor-1}(\frac{1+\sqrt{p}}{2})=\frac{(\sqrt{p-1}-1)+\sqrt{p}}{2}$

Using Lemma 2.1 (Malik *et al*., 2004) we have $(xy^3)(xy)^{\lfloor\frac{\sqrt{p-1}}{2}\rfloor-1}(\frac{1+\sqrt{p}}{2})=\frac{(\sqrt{p-1}-3)+\sqrt{p}}{3\sqrt{p-1}-4}$

Using Lemma 3.6 we obtain $(xy^5)^{\lfloor\frac{\sqrt{p-1}}{2}\rfloor-1}(xy^3)(xy)^{\lfloor\frac{\sqrt{p-1}}{2}\rfloor-1}(\frac{1+\sqrt{p}}{2})=\frac{(3-\sqrt{p-1})+\sqrt{p}}{3\sqrt{p-1}-4}$

. Using Lemma 2.1 (Malik *et al*., 2004) we have

$(xy^3)(xy^5)^{\lfloor\frac{\sqrt{p-1}}{2}\rfloor-1}(xy^3)(xy)^{\lfloor\frac{\sqrt{p-1}}{2}\rfloor-1}(\frac{1+\sqrt{p}}{2})=\frac{(1-\sqrt{p-1})+\sqrt{p}}{2}$

Using Lemma 3.6 we obtain

$(xy)^{\lfloor\frac{\sqrt{p-1}}{2}\rfloor}(xy^3)(xy^5)^{\lfloor\frac{\sqrt{p-1}}{2}\rfloor-1}(xy^3)(xy)^{\lfloor\frac{\sqrt{p-1}}{2}\rfloor-1}(\frac{1+\sqrt{p}}{2})=(\frac{1+\sqrt{p}}{2})$

. Hence The circuit of $(\frac{1+\sqrt{p}}{2})^M$ have the type

$((\lfloor\frac{\sqrt{p-1}}{2}\rfloor)_0,1_2,(\lfloor\frac{\sqrt{p-1}}{3}\rfloor-1)_4,1_2,(\lfloor\frac{\sqrt{p-1}}{2}\rfloor-1)_0)$

and hence have ambiguous length $\frac{8}{3}\sqrt{p-1}$. First part can be proved similarly.□

Example 3.11 1. Let $p=37$. Then by Theorem 3.10, the element of M that fixes $\alpha=\sqrt{37}$ and its conjugate is $(xy)^6(xy^5)^4(xy)^6$, the circuit of $(\frac{\sqrt{37}}{1})^M$ and its conjugate have the type $(6_0,4_4,6_0)$ and $|(\frac{\sqrt{p}}{1})^M|_{amb}=32=|(\frac{\sqrt{p}}{-1})^M|_{amb}$.

2. The element of M that fixes $\beta=\frac{1+\sqrt{p}}{2}$ and its conjugate is $(xy)^3(xy^3)(xy^5)(xy^3)(xy)^2$, the circuit of $(\frac{1+\sqrt{p}}{2})^M$ and its conjugate have the type $(2_0,1_2,1_4,1_2,3_0)$ and $|(\frac{1+\sqrt{p}}{2})^M|_{amb}=16=|(\frac{-1+\sqrt{p}}{-2})^M|_{amb}$. ♦

Theorem 3.12 Let $p\equiv 5(mod\ 12)$ such that $p-4=\lfloor\sqrt{p}\rfloor^2$. Then:

1. $|(\frac{\sqrt{p}}{1})^M|_{amb}=2(6\sqrt{p-4}+2)=|(\frac{\sqrt{p}}{-1})^M|_{amb}$
2. $|(\frac{-1+\sqrt{p}}{-2})^M|_{amb}=4\sqrt{p-4}=|(\frac{-1+\sqrt{p}}{-2})^M|_{amb}$

Proof: The proof is Straightforward.□

4 M -Orbits of $Q^{*\sim}(\sqrt{9p})$, $p\equiv 1(mod\ 4)$ with $o^{*\sim}_M(p)>4$

Let $p\equiv 1(mod\ 4)$. If

$|(\sqrt{p})^M|_{amb}+|(\frac{\sqrt{p}}{-1})^M|_{amb}+|(\frac{1+\sqrt{p}}{2})^M|_{amb}+|(\frac{-1+\sqrt{p}}{-2})^M|_{amb}=|Q^{*\sim}(\sqrt{9p})|$

,

Then we have $o^{*\sim}_M(p)=4$. If

$|(\sqrt{p})^M|_{amb}+|(\frac{\sqrt{p}}{-1})^M|_{amb}+|(\frac{1+\sqrt{p}}{2})^M|_{amb}+|(\frac{-1+\sqrt{p}}{-2})^M|_{amb}<|Q^{*\sim}(\sqrt{9p})|$

Then we have the following results.

Lemma 4.1 Let $n\equiv 1(mod\ 4)$. Then:

1 $(\alpha)^M\cap(\overline{\alpha})^M=\varnothing$ for all $\alpha\in Q^{*\sim}(\sqrt{9n})\setminus((\sqrt{n})^M\cup(\frac{\sqrt{n}}{-1})^M\cup(\frac{1+\sqrt{n}}{2})^M\cup(\frac{-1+\sqrt{n}}{-2})^M)$

.

2. $(\alpha)^M\cap(-\alpha)^M=\varnothing$ for all $\alpha\in Q^{*\sim}(\sqrt{9n})\setminus((\sqrt{n})^M\cup(\frac{\sqrt{n}}{-1})^M\cup(\frac{1+\sqrt{n}}{2})^M\cup(\frac{-1+\sqrt{n}}{-2})^M)$

Proof: By Malik *et al*., 1995, we know that $\frac{a+\sqrt{n}}{\pm c},\frac{-a+\sqrt{n}}{\pm c}$ are contained in $(\sqrt{n})^M$ *or* $(\frac{\sqrt{n}}{-1})^M$ where $c\not\equiv 0(mod\ 3)$ and $\frac{c+\sqrt{n}}{\pm a},\frac{-c+\sqrt{n}}{\pm a}$ are contained in $(\frac{1+\sqrt{n}}{2})^M$ *or* $(\frac{-1+\sqrt{n}}{-2})^M$ where $a\not\equiv 0(mod\ 3)$.

Hence using Lemma 1.10 we have $(\alpha)^M\cap(\overline{\alpha})^M=\varnothing$ for all $\alpha\in Q^{*\sim}(\sqrt{9n})\setminus((\sqrt{n})^M\cup(\frac{\sqrt{n}}{-1})^M\cup(\frac{1+\sqrt{n}}{2})^M\cup(\frac{-1+\sqrt{n}}{-2})^M)$

The 2nd part directly follows by Theorem 1.6 (Malik *et al*., 2012).□

In the following lemma we use $Q'''(\sqrt{n})=Q'(\sqrt{n})\cup\frac{1}{3}Q'(\sqrt{n})$.

Lemma 4.2 Let $n\equiv 1(mod\ 4)$. Then:

$\frac{1+\sqrt{n}}{4}\in Q''''(\sqrt{n})\ or\ Q^{*\sim}(\sqrt{9n})\setminus Q''''(\sqrt{n})$

according as $n\equiv 1\ or\ 17(mod\ 24)$ or $n\equiv 5\ or\ 13(mod\ 24)$

Proof: The proof is straightforward.

Lemma 4.3 Let $p \equiv 5(mod\ 12)$ such that $p-1$ is a perfect square. If

$$(Q^{*\sim}(\sqrt{9p}) \setminus Q''''(\sqrt{p})) \setminus ((\sqrt{p})^M \cup (\frac{\sqrt{p}}{-1})^M) \neq \varnothing$$

, then either

$$\frac{1+\sqrt{p}}{q_1} \text{ or } \frac{2+\sqrt{p}}{t_1} \in (Q^{*\sim}(\sqrt{9p}) \setminus Q''''(\sqrt{p})) \setminus ((\sqrt{p})^M \cup (\frac{\sqrt{p}}{-1})^M)$$

.

Proof: Using Remark 3.9,

$$(\sqrt{p})^M \cup (\frac{\sqrt{p}}{-1})^M = \{\frac{\pm a+\sqrt{p}}{\pm 1}, \frac{\pm a+\sqrt{p}}{\pm (p-a^2)}, 0 \le a \le \lfloor \sqrt{p} \rfloor\}$$

. If

$$(Q^{*\sim}(\sqrt{9p}) \setminus Q''''(\sqrt{p})) \setminus ((\sqrt{p})^M \cup (\frac{\sqrt{p}}{-1})^M) \neq \varnothing$$

, then either $p-1$ is not power of two or is power of 2 using Remark 3.6 [?]. In first case $p-1$ is not power of two then there exists

$$\frac{1+\sqrt{p}}{q_1} \in (Q^{*\sim}(\sqrt{9p}) \setminus Q''''(\sqrt{p})) \setminus ((\sqrt{p})^M \cup (\frac{\sqrt{p}}{-1})^M)$$

. If $p-1$ is power of 2 then $p-4$ is not power of 2. Thus there exists

$$\frac{2+\sqrt{p}}{t_1} \in (Q^{*\sim}(\sqrt{9p}) \setminus Q''''(\sqrt{p})) \setminus ((\sqrt{p})^M \cup (\frac{\sqrt{p}}{-1})^M)$$

. W

Corollary 4.4 Let $p \equiv 5(mod\ 12)$ such that $p-1$ is a perfect square. If

$$(Q^{*\sim}(\sqrt{9p}) \setminus Q''''(\sqrt{p})) \setminus ((\sqrt{p})^M \cup (\frac{\sqrt{p}}{-1})^M) \neq \varnothing$$

, then

$$(\sqrt{p})^M \cup (\frac{\sqrt{p}}{-1})^M \cup (\frac{1+\sqrt{p}}{q_1})^M \cup (\frac{-1+\sqrt{p}}{q_1})^M \cup (\frac{1+\sqrt{p}}{-q_1})^M \cup (\frac{-1+\sqrt{p}}{-q_1})^M \subseteq Q^{*\sim}(\sqrt{9p})$$

or

$$(\sqrt{p})^M \cup (\frac{\sqrt{p}}{-1})^M \cup (\frac{2+\sqrt{p}}{t_1})^M \cup (\frac{-2+\sqrt{p}}{t_1})^M \cup (\frac{2+\sqrt{p}}{-t_1})^M \cup (\frac{-2+\sqrt{p}}{-t_1})^M \subseteq Q^{*\sim}(\sqrt{9p})$$

Proof: The proof is straightforward and follows by Lemma 4.3.□

Lemma 4.5 Let $p \equiv 17(mod\ 24)$ such that $p-1$ is a perfect square. Then $Q^{*\sim}(\sqrt{9p})$ splits into atleast twelve M -orbits for $p > 17$

Proof: Using Remark 3.9,

$$(\sqrt{p})^M_{amb} \cup (\frac{\sqrt{p}}{-1})^M_{amb} = \{\frac{\pm a+\sqrt{p}}{\pm 1}, \frac{\pm a+\sqrt{p}}{\pm (p-a^2)}, 0 \le a < \lfloor \sqrt{p} \rfloor\}$$

and

$$(\frac{1+\sqrt{p}}{2})^M_{amb} \cup (\frac{-1+\sqrt{p}}{-2})^M_{amb} = \{\frac{\pm a+\sqrt{p}}{\pm 2}, \frac{\pm a+\sqrt{p}}{\frac{p-a^2}{\pm 2}}, \frac{\pm 1+\sqrt{p}}{\pm \lfloor \sqrt{p} \rfloor} : a = 1,3,.. \lfloor \sqrt{p} \rfloor - 1\}$$

Also $(\sqrt{p})^M \cup (\frac{\sqrt{p}}{-1})^M \subseteq Q^{*\sim}(\sqrt{9p}) \setminus Q''''(\sqrt{p})$

and $(\frac{1+\sqrt{p}}{2})^M \cup (\frac{-1+\sqrt{p}}{-2})^M \subseteq Q''''(\sqrt{p})$.

For $p > 17$ we have atleast four more M -orbits namely $(\frac{\pm 1+\sqrt{p}}{\pm 4})^M$ contained in $Q''''(\sqrt{p})$ since otherwise $\lfloor \sqrt{p} \rfloor = 4$ and hence $\frac{\pm 1+\sqrt{p}}{\pm 4} \in (\frac{1+\sqrt{p}}{2})^M \cup (\frac{-1+\sqrt{p}}{-2})^M$.

Hence For $p > 17$, $\frac{\pm 1+\sqrt{p}}{\pm 4} \notin (\frac{1+\sqrt{p}}{2})^M \cup (\frac{-1+\sqrt{p}}{-2})^M$. This shows $Q''''(\sqrt{p})$ contains atleast six M -orbits.

By Corollary 4.4 we have six M -orbits either

$$(\sqrt{p})^M \cup (\frac{\sqrt{p}}{-1})^M \cup (\frac{1+\sqrt{p}}{q_1})^M \cup (\frac{-1+\sqrt{p}}{q_1})^M \cup (\frac{1+\sqrt{p}}{-q_1})^M \cup (\frac{-1+\sqrt{p}}{-q_1})^M$$

or

$$(\sqrt{p})^M \cup (\frac{\sqrt{p}}{-1})^M \cup (\frac{2+\sqrt{p}}{t_1})^M \cup (\frac{-2+\sqrt{p}}{t_1})^M \cup (\frac{2+\sqrt{p}}{-t_1})^M \cup (\frac{-2+\sqrt{p}}{-t_1})^M$$

contained in $Q^{*\sim}(\sqrt{9p}) \setminus Q''''(\sqrt{p})$. Thus we have atleast twelve M -orbits.

Lemma 4.6 Let $p \equiv 5 \text{ or } 13(mod\ 24)$ such that $p-1$ is a perfect square. Then $Q^{*\sim}(\sqrt{9p})$ splits into atleast eight M -orbits for $p > 13$

Proof: Using Lemma 4.2, $\frac{1+\sqrt{n}}{4} \in Q^{*\sim}(\sqrt{9n}) \setminus Q''''(\sqrt{n})$. Also $(\sqrt{p})^M \cup (\frac{\sqrt{p}}{-1})^M \subseteq Q^{*\sim}(\sqrt{9p}) \setminus Q''''(\sqrt{p})$. For $p > 13$, $\frac{\pm 1+\sqrt{p}}{\pm 4} \notin (\sqrt{p})^M \cup (\frac{\sqrt{p}}{-1})^M$ otherwise

for $p=13, \frac{\pm 1+\sqrt{13}}{\pm 4} \in (\sqrt{13})^M \cup (\frac{\sqrt{13}}{-1})^M$ hence $(\frac{\pm 1+\sqrt{p}}{\pm 4})^M$ exists and contained in $Q^{*\sim}(\sqrt{9n}) \setminus Q''''(\sqrt{n})$. Thus

$$(\sqrt{p})^M \cup (\frac{\sqrt{p}}{-1})^M \cup (\frac{1+\sqrt{n}}{4})^M \cup (\frac{-1+\sqrt{n}}{4})^M \cup (\frac{1+\sqrt{n}}{-4})^M \cup (\frac{-1+\sqrt{n}}{-4})^M \subseteq Q^{*\sim}(\sqrt{9n}) \setminus Q''''(\sqrt{n})$$

and $(\frac{1+\sqrt{p}}{2})^M \cup (\frac{-1+\sqrt{p}}{-2})^M \subseteq Q''''(\sqrt{n})$.

Hence we have eight M -orbits. □

Example 4.7 Let $p=37$. By Theorem $3.1, Q^{*\sim}(\sqrt{9p})$ splits in atleast four M -orbits, namely,

$(\sqrt{p})^M, (\frac{\sqrt{p}}{-1})^M, (\frac{1+\sqrt{p}}{2})^M$ *and* $(\frac{-1+\sqrt{p}}{-2})^M$.

By Theorem 3.6, $|(\frac{\sqrt{p}}{\pm 1})^M|_{amb}=32$ and $|(\frac{1\pm\sqrt{p}}{2})^M|_{amb}=16$, $|Q_1^*(\sqrt{37})|=124$ and using Theorem 1.10, $|Q_1^{***}(\sqrt{37})|=52$. Using Theorem 2.4, $|Q_1^{*\sim}(\sqrt{9.37})|=2(124-52)=144$. Since $|(\sqrt{p})^M|_{amb}+|(\frac{\sqrt{p}}{-1})^M|_{amb}+|(\frac{1+\sqrt{p}}{2})^M|_{amb}+|(\frac{-1+\sqrt{p}}{-2})^M|_{amb}=96<144$ .Therefore by Lemmas 4.2 and 4.3 atleast four more M -orbits exists which are $(\frac{\pm 1+\sqrt{37}}{\pm 4})^M$. Also $|(\frac{\pm 1+\sqrt{37}}{\pm 4})^M|_{amb}=12$. Here the sum of cardinalities of all eight orbits is 144. Therefore we conclude that $Q^{*\sim}(\sqrt{9.37})$ splits into exactly eight M -orbits.

Lemma 4.8 Let $p \equiv 1(mod\ 24)$ such that $p-1$ is a perfect square.Then $Q^{*\sim}(\sqrt{9p})$ splits into atleast eight M -orbits.

Proof: Using Remark 3.5,

$$(\sqrt{p})^M_{amb} \cup (\frac{\sqrt{p}}{-1})^M_{amb} = \{\frac{\pm a+\sqrt{p}}{\pm 1}, \frac{\pm a+\sqrt{p}}{\pm(p-a^2)}, 0 \le a \le \lfloor\sqrt{p}\rfloor$$

where $p-a^2 \not\equiv 0(mod\ 3)\}$ and

$$(\frac{1+\sqrt{p}}{2})^M_{amb} \cup (\frac{-1+\sqrt{p}}{-2})^M_{amb} = \{\frac{\pm a+\sqrt{p}}{\pm 2}, \frac{\pm a+\sqrt{p}}{\frac{p-a^2}{\pm 2}} : a=1,3,.\lfloor\sqrt{p}\rfloor-1 \text{ where } p-a^2 \not\equiv 0(mod\ 3)\}$$

Also $(\sqrt{p})^M \cup (\frac{\sqrt{p}}{-1})^M \subseteq Q^{*\sim}(\sqrt{9p}) \setminus Q''''(\sqrt{p})$

and $(\frac{1+\sqrt{p}}{2})^M \cup (\frac{-1+\sqrt{p}}{-2})^M \subseteq Q''''(\sqrt{p})$.

$\frac{1+\sqrt{p}}{4} \notin (\frac{1+\sqrt{p}}{2})^M \cup (\frac{-1+\sqrt{p}}{-2})^M$ for $p \equiv 1(mod\ 24)$ such that $p-1$ is a perfect square. Since $\frac{1+\sqrt{p}}{4} \in Q''''(\sqrt{n})$. Thus we have four more M -orbits and conclude that $Q^{*\sim}(\sqrt{9p})$ splits into atleast eight M -orbits.□

Example 4.9 Let $p=577$. Then $Q^{*\sim}(\sqrt{9.577})$ splits into at least twenty M -orbits, namely, $(\frac{577}{1})^M$, $(\frac{577}{-1})^M$, $(\frac{1+\sqrt{577}}{2})^M$, $(\frac{-1+\sqrt{577}}{-2})^M$, $(\frac{1+\sqrt{577}}{4})^M$, $(\frac{-1+\sqrt{577}}{4})^M$, $(\frac{1+\sqrt{577}}{-4})^M$, $(\frac{-1+\sqrt{577}}{-4})^M$, $(\frac{1+\sqrt{577}}{8})^M$, $(\frac{-1+\sqrt{577}}{8})^M$, $(\frac{1+\sqrt{577}}{-8})^M$, $(\frac{-1+\sqrt{577}}{-8})^M$, $(\frac{1+\sqrt{577}}{16})^M$, $(\frac{-1+\sqrt{577}}{16})^M$, $(\frac{1+\sqrt{577}}{-16})^M$, $(\frac{-1+\sqrt{577}}{-16})^M$, $(\frac{3+\sqrt{577}}{8})^M$, $(\frac{-3+\sqrt{577}}{8})^M$, $(\frac{3+\sqrt{577}}{-8})^M$ and $(\frac{-3+\sqrt{577}}{-8})^M$.

Lemma 4.10 Let $p \equiv 5(mod\ 12)$ such that $p-1$ is a perfect square. Then $p \equiv 17\ or\ 5(mod\ 24)$ according as $\lfloor\sqrt{p}\rfloor \equiv 0\ or\ 2(mod\ 4)$.

Proof: The proof is straightforward.□

Remark 4.11 For $p \equiv 5(mod\ 24)$ such that $p-1$ is a perfect square.

1. Let $Y = \{\frac{\pm 1+\sqrt{p}}{\pm c} \in Q^*(\sqrt{p}) : c = 1, \lfloor\sqrt{p}\rfloor^2\}$

2. Let $Z = \{\frac{\pm 1+\sqrt{p}}{\pm c} \in Q^*(\sqrt{p}) : c = 1, \frac{\lfloor\sqrt{p}\rfloor^2}{2}, \lfloor\sqrt{p}\rfloor\}$

Then $Y \cup x(Y) \subseteq (\sqrt{p})^M \cup (\frac{\sqrt{p}}{-1})^M$ and $Z \cup x(Z) \subseteq (\frac{1+\sqrt{p}}{2})^M \cup (\frac{-1+\sqrt{p}}{-2})^M$.□

Theorem 4.12 Let $p \equiv 5(mod\ 24)$ such that $p-1 = \lfloor\sqrt{p}\rfloor^2 = (2q_1)^2$. Then:

$|(\frac{1+\sqrt{p}}{4})^M|_{amb} = |(\frac{-1+\sqrt{p}}{4})^M|_{amb} = |(\frac{1+\sqrt{p}}{-4})^M|_{amb} = |(\frac{-1+\sqrt{p}}{-4})^M|_{amb} = 2\sqrt{p-1}+12$

Proof: The proof is analogous to Theorem 3.4.□

Remark 4.13 Let $p \equiv 5(mod\ 24)$ such that $p-1 = \lfloor\sqrt{p}\rfloor^2 = (2q_1)^2$. Then:

$(\frac{1+\sqrt{p}}{4})^M = (\frac{1+\sqrt{p}}{q_1})^M$.□

Remarks 4.14 It can be easily seen by Malik and Aneesa, 2011, Theorem 3.2 and Remark 3.3 that:

- 257 and 761 are the only primes $p \equiv 17(mod\ 24)$ and $p < 2011$ such that $o_M(p) = 12$.
- 401 and 1601 are the only primes $p \equiv 17(mod\ 24)$ and $p < 2011$ such that $o_M(p) > 12$

For $p = 401$, $Q''(\sqrt{p})$ splits into twenty M -orbits, namely, $(\frac{\sqrt{p}}{1})^M$, $(\frac{\sqrt{p}}{-1})^M$, $(\frac{1+\sqrt{p}}{2})^M$, $(\frac{-1+\sqrt{p}}{-2})^M$, $(\frac{1+\sqrt{p}}{4})^M$, $(\frac{1+\sqrt{p}}{-4})^M$, $(\frac{-1+\sqrt{p}}{4})^M$, $(\frac{-1+\sqrt{p}}{-4})^M$, $(\frac{1+\sqrt{p}}{5})^M$, $(\frac{-1+\sqrt{p}}{5})^M$, $(\frac{1+\sqrt{p}}{-5})^M$, $(\frac{-1+\sqrt{p}}{-5})^M$, $(\frac{1+\sqrt{p}}{8})^M$, $(\frac{1+\sqrt{p}}{-8})^M$, $(\frac{-1+\sqrt{p}}{8})^M$, $(\frac{-1+\sqrt{p}}{-8})^M$, $(\frac{1+\sqrt{p}}{16})^M$, $(\frac{-1+\sqrt{p}}{16})^M$, $(\frac{1+\sqrt{p}}{-16})^M$ and $(\frac{-1+\sqrt{p}}{-16})^M$.

For $p = 1601$, $Q''(\sqrt{p})$ splits into twenty eight M -orbits, namely, $(\frac{\sqrt{p}}{1})^M$, $(\frac{\sqrt{p}}{-1})^M$, $(\frac{1+\sqrt{p}}{2})^M$, $(\frac{-1+\sqrt{p}}{-2})^M$, $(\frac{1+\sqrt{p}}{4})^M$, $(\frac{1+\sqrt{p}}{-4})^M$, $(\frac{-1+\sqrt{p}}{4})^M$, $(\frac{-1+\sqrt{p}}{-4})^M$, $(\frac{1+\sqrt{p}}{5})^M$, $(\frac{-1+\sqrt{p}}{5})^M$, $(\frac{1+\sqrt{p}}{-5})^M$, $(\frac{-1+\sqrt{p}}{-5})^M$, $(\frac{1+\sqrt{p}}{8})^M$, $(\frac{1+\sqrt{p}}{-8})^M$, $(\frac{-1+\sqrt{p}}{8})^M$, $(\frac{-1+\sqrt{p}}{-8})^M$, $(\frac{1+\sqrt{p}}{16})^M$, $(\frac{-1+\sqrt{p}}{16})^M$, $(\frac{1+\sqrt{p}}{-16})^M$, $(\frac{-1+\sqrt{p}}{-16})^M$, $(\frac{1+\sqrt{p}}{25})^M$, $(\frac{-1+\sqrt{p}}{25})^M$, $(\frac{1+\sqrt{p}}{-25})^M$, $(\frac{-1+\sqrt{p}}{-25})^M$, $(\frac{3+\sqrt{p}}{8})^M$, $(\frac{-3+\sqrt{p}}{8})^M$, $(\frac{3+\sqrt{p}}{-8})^M$ and $(\frac{-3+\sqrt{p}}{-8})^M$.

- The primes $p \equiv 5(mod\ 24)$ and $p < 2011$ such that $o_M(p) = 8$ are $101, 197, 269, 389, 557, 677, 701, 1301, 1613, 1949$ and 1973.
- For $p = 1901$, $Q''(\sqrt{p})$ splits into twenty four M -orbits, namely, $(\frac{\sqrt{p}}{1})^M$, $(\frac{\sqrt{p}}{-1})^M$, $(\frac{1+\sqrt{p}}{2})^M$, $(\frac{-1+\sqrt{p}}{-2})^M$, $(\frac{1+\sqrt{p}}{4})^M$, $(\frac{1+\sqrt{p}}{-4})^M$,

$(\frac{-1+\sqrt{p}}{4})^M$, $(\frac{-1+\sqrt{p}}{-4})^M$, $(\frac{1+\sqrt{p}}{5})^M$, $(\frac{-1+\sqrt{p}}{5})^M$, $(\frac{1+\sqrt{p}}{-5})^M$, $(\frac{-1+\sqrt{p}}{-5})^M$, $(\frac{1+\sqrt{p}}{10})^M$, $(\frac{1+\sqrt{p}}{-10})^M$, $(\frac{-1+\sqrt{p}}{10})^M$, $(\frac{-1+\sqrt{p}}{-10})^M$, $(\frac{1+\sqrt{p}}{19})^M$, $(\frac{-1+\sqrt{p}}{19})^M$, $(\frac{1+\sqrt{p}}{-19})^M$, $(\frac{-1+\sqrt{p}}{-19})^M$, $(\frac{1+\sqrt{p}}{25})^M$, $(\frac{-1+\sqrt{p}}{25})^M$, $(\frac{1+\sqrt{p}}{-25})^M$ and $(\frac{-1+\sqrt{p}}{-25})^M$. It is also noted that 1901 is the only prime $p \equiv 5(mod\ 24)$ and $p < 2011$ such that $o_M(p) > 12$.

- The following are the primes $p \equiv 13(mod\ 24)$ and $p < 2011$ such that $o_M^{*\sim}(p) = 8$: 37,349,373,709,757,829,877,997,1213 and 1861.

REFERENCES

Andrew Adler, John E. Coury, *The Theory of Numbers*, (Jones and Bartlett, Inc. 1995).

Mushtaq Q. Modular Group acting on Real Quadratic Fields. Bull. Austral. Math. Soc. Vol. 37, (1988), 303-309, 89e:11065.

Malik M. A., S. M. Husnine and A. Majeed. Modular group action on Certain Quadratic Fields. PUJM, Vol. 28 (1995), 47-68

Mushtaq Q., M. Aslam. Group generated by two elements of orders two and six acting on R and $Q(\sqrt{m})$. Discrete Mathematics 179 (1998), 145-154.

Malik M. A., S. M. Husnine and A. Majeed. The Orbits of $Q^*(\sqrt{p}), p \equiv 1(mod\ 4)\ or\ p = 2$ under the action of Modular Group. PUJM, Vol. 33 (2000), 37-50. (Stefein Kunlein)Mr. 2002M:11031 11F06.

Malik M. A., S. M. Husnine and A. Majeed. The Orbits of $Q^*(\sqrt{p}), p \equiv 3(mod\ 4)$ under the action of Modular Group $G = \langle x^2, y : x = y^3 = 1 \rangle$. PUJM, vol. 37, (2003-4), 1-14.

Malik M. A., S. M. Husnine and A. Majeed. Action of The group $M = \langle x, y : x^2 = y^6 = 1 \rangle$ on Certain Real Quadratic Fields. PUJM, Vol. 36 (2003-04), 71-88

Malik M. A., S. M. Husnine and A. Majeed. On ambiguous numbers of an invariant subset $Q^*(\sqrt{k^2 m})\ of\ Q(\sqrt{m})$ under the action of the Modular Group PSL(2,Z). Studia Scientiarum Mathematicarum Hungarica vol. 42 (4) (2005), 401-412

Malik M. A., S. M. Husnine and A. Majeed. Action of the Mobius Group $M = \langle x, y : x^2 = y^6 = 1 \rangle$ on Certain Real Quadratic Fields (accepted)

Mushtaq Q. Reduced Indefinite binary quadratic forms and orbits of the modular group, Radovi Mathematicki Vol. 4 (1988), 331-336.

Kouser I., S. M. Husnine and A. Majeed. Equivalent binary quadratic forms and the Orbits of $Q^*(\sqrt{p})$ under the action of the Modular Group. PUJM, Vol. 33 (2000), 125-134.

Malik M. A., Aneesa Mughal. Transitive G-subsets of an invariant subset $Q^*(\sqrt{p})\ of\ Q(\sqrt{p}), p \equiv 1(mod\ 4)$ (submitted) 2011.

Malik M. A., Aneesa Mughal. Transitive G-subsets of an invariant subset $Q^*(\sqrt{p})\ of\ Q(\sqrt{p}), p \equiv 3(mod\ 4)$ (submitted) 2012.

Mushtaq Q. Modular Group Acting on Real Quadratic Fields. Bull. Austral. Math. Soc. Vol. 37, (1988), 303-309, 89e:11065

Malik M. A., M. Asim Zafar. Real quadratic irrational numbers and Modular Group Action. Southeast Asian Bulletin of Mathematics Vol. 35 (3) (2011), 439-445.

Zia T. J., G. Q. Abbasi. Action of Subgroups of $H = \langle x, y : x^2 = y^4 = 1 \rangle$ on $Q^*(\sqrt{n})$, Journal of Applied Sciences, Vol. 6 (8) (2006), 1720-1724.

Aslam M., Q. Mushtaq. Closed paths in the coset diagrams for $\langle y, t : y^6 = t^6 = 1 \rangle$ acting on Real Quadratic Fields. Ars Comb. Vol. 71, (2004) 741-748.