A GENERALIZED CLASSIFICATION AND ENUMERATION OF ORBITS OF $Q^*(\sqrt{n}\ )$ BY $PSL(2,Z)$

M. Khalid Mahmood[1], Yaser Daanial Khan[2]

Several attempts have been made to find orbits of invariant sets under the action of projective special linear groups using coset diagrams. We present a novel approach to resolve the problem for the enumeration of $PSL(2,Z)$-orbits using its invariant set $Q^*(\sqrt{n}\ )$. The proposed technique is free from coset diagram and is less computationally intensive as compared to its existing techniques. Let $g = \prod_{i=1}^{r} p_i^{k_i},\ k_i \geq 1$, where $p_1, p_2, ..., p_r$ are distinct odd primes. The cardinality of the the set E_g, consisting of all classes $[a,b,c]$ mod g, of the elements in $Q^*(\sqrt{n}\ )$ has been determined and shown to be equal to $g^3 \prod_{i=1}^{r}(1-\frac{1}{p_i^3})$. Finally, we use classification and propose algorithms to enumerate $PSL(2,Z)$-orbits of $Q^*(\sqrt{n}\ )$.

Keywords: Classification, Quadratic congruence, G-Orbits.//05C25, 11E04,20G15.

MSC2010: 05C25, 11E04,20G15.

1. Introduction

It is well known that every real quadratic irrational number $u + v\sqrt{m}$ of $Q(\sqrt{m})$ can be written uniquely as $\frac{a+\sqrt{n}}{c}$, where n is a non-square positive integer and $(a,b,c) = 1,\ b = \frac{a^2-n}{c}$. Let $g > 1$ be a fixed integer. Two classes $\alpha(a,b,c)$ and $\alpha'(a',b',c')$ of $Q^*(\sqrt{n})$ are g-equivalent if and only if $a \equiv a' \pmod{g}$, $b \equiv b' (\text{mod } g)$ and $c \equiv c' \pmod{g}$, where $\alpha = \frac{a+\sqrt{n}}{c}$ is assigned by $\alpha(a,b,c)$. Since the congruence relation partitions set of integers into disjoint classes, so the equivalence classes $[a,b,c] \pmod{g}$ for each $g > 1$ can be determined. The set E_g denote the collection of all such classes $[a,b,c]$ modulo g and the set of all classes $[a,b,c] \pmod{g}$ of the elements of $Q^*(\sqrt{n})$ with $n \equiv i \pmod{g}$ is labeled by E_g^i (or E_g^n,) where $i = 0, 1, ..., g-1$. Define the algebraic conjugate of α as $\bar{\alpha} = \frac{a-\sqrt{n}}{c}$. A number is called ambiguous if it is of opposite sign then its conjugate. These numbers play a significant role in studying the action of G on the field $Q(\sqrt{m})$.

Define the modular group $G = \langle x, y : x^2 = y^3 = 1\rangle$ where, $x : \alpha \to \frac{-1}{\alpha}$ and $y : \alpha \to \frac{\alpha-1}{\alpha}$ are the linear fractional transformations. Coset diagrams for $PSL(2,Z)$-orbits of $Q^*(\sqrt{n})$ have been used earlier. In [4], an explicit formula to enumerate the finite ambiguous numbers in $Q^*(\sqrt{n})$, has been established. Further it is shown that the ambiguous numbers are the vertices of a closed path, the orbit α^G. A closed form expression as a function of n for the ambiguous numbers in $Q^*(\sqrt{n})$ has been given in [4]. In [3], the cardinality of the set $E_p^r,\ r \geq 1$ of the elements in $Q^*(\sqrt{n}\ )$ and few of its $G-$subsets have been determined for a single prime power. The motivation behind the proposed research work is to generalize the results regarding the cardinality of the set E_n, corresponding to every odd

[1] Assistant Professor, Department of Mathematics, University of the Punjab, Lahore, Pakistan, e-mail: khalid.math@pu.edu.pk

[2] Assistant Professor, Faculty of Information Technology, University of Management and Technology, Lahore, Pakistan

integer n. Moreover, we note that the exposition of G-orbits through coset diagrams seemed to be strenuous and much more laborious. So an attempt is made to keep the elucidation at a consistently low level to get advantage in finding the desired orbits directly.

In this article, an account of classifications of the set $Q^*(\sqrt{n})$ in terms of finite number of classes has been provided. Let $g = \prod_{i=1}^{r} p_i^{k_i},\ k_i \geq 1$ and $p_1, p_2, ..., p_r$ are distinct odd primes. The cardinality of the the set E_g, consisting of all classes $[a, b, c]$ mod g, of the elements in $Q^*(\sqrt{n}\ )$ has been determined and shown to be equal to $g^3 \prod_{i=1}^{r}(1 - \frac{1}{p_i^3})$. It is shown that if $g \mid n$ then $|E_g^n| \leq \sigma(g)\phi(g)$, where ϕ is the Euler's phi function and σ denote the sum of positive divisors of $g = \prod_{i=1}^{r} p_i^{k_i}$. As an application, the classes for ambiguous numbers to study the G-orbits of $Q^*(\sqrt{n})$ has been scrutinized. Hence by using these ambiguous numbers, enumeration for the orbits of $Q^*(\sqrt{n})$ under the action of the modular group G have been resolved. Notations used in this paper are standard which follow [1, 2, 3, 4] and [6]. In particular, $\left(\frac{a}{p}\right)$ denotes the Legender of a modulo p.

2. Some Previous Results

In this section few of the previous results have been given so as to make this paper self contained.

Theorem 2.1. [1] Let q be a an odd prime, m any integer such that $q \nmid m$, and n any positive integer. Then, $x^2 \equiv m \pmod{p^n}$ has a solution if and only if $\left(\frac{m}{q}\right) = 1$.

Theorem 2.2. [1] Let $g(x)$ be a polynomial over integers, and suppose, $N(q)$ is the number of incongruent integers satisfying $g(x) \equiv 0 \pmod{q}$. If $q = q_1q_2$ where $(q_1, q_2) = 1$, then $N(q) = N(q_1)N(q_2)$. If $q = \prod q_i^{\alpha_i}$ is the prime factorization of q, then $N(q) = \prod N(q_i^{\alpha_i})$.

Theorem 2.3. [1] Let m be a positive integer with canonical decomposition $2^{e_0} \prod p_i^{e_i}$ and a any integer with $(a, m) = 1$. Then $x^2 \equiv a \pmod{m}$ has a solution if and only if $x^2 \equiv a \pmod{2^{e_0}}$ and $x^2 \equiv a \pmod{p_i^{e_i}}$ are solvable.

Theorem 2.4. [2, 3] Let p be an odd prime, Then.

(i)

$$|E_{p^k}^n| = \begin{cases} p^{2(k-1)}(p^2 - 1), & \text{if } p \mid n \\ p^{2(k-1)}p(p - 1), & \left(\frac{n}{p}\right) = -1 \\ p^{2(k-1)}p(p + 1), & \left(\frac{n}{p}\right) = 1 \end{cases}$$

(ii) $|\bigcup_{j=0}^{p-1} E_j^n| = p^3 - 1$.

3. Classification of the elements of $Q^*(\sqrt{n})$

The following lemma gives the cardinality of the classes $[a, b, c] \pmod{g}$ where g is a product of two distinct odd primes.

Lemma 3.1. Let p_1 and p_2 be distinct odd primes.

$$|E_{p_1p_2}^n| = \begin{cases} (p_1^2 - 1)(p_2^2 - 1), & \text{if } p_1 \mid n \text{ and } p_2 \mid n \\ p_1p_2(p_1 + 1)(p_2 + 1), & \left(\frac{n}{p_1}\right) = 1 \text{ and } \left(\frac{n}{p_2}\right) = 1 \\ p_1p_2(p_1 - 1)(p_2 - 1), & \left(\frac{n}{p_1}\right) = -1 \text{ and } \left(\frac{n}{p_2}\right) = -1 \\ p_1p_2(p_1 + 1)(p_2 - 1), & \left(\frac{n}{p_1}\right) = 1 \text{ and } \left(\frac{n}{p_2}\right) = -1 \end{cases}$$

The proof of the above Lemma is analogous to Theorem 2.3.

Let $p_1, p_2, ..., p_r$ be distinct odd primes and $g = \prod_{i=1}^{r} p_i^{k_i}$. To find the cardinality $|\bigcup_{j=0}^{g-1} E_g^n|$, where $n \equiv j\ (mod\ g)$ and $j = 0, 1, 2, ..., \overline{g-1}$, we give the following theorems.

Theorem 3.1. Let p_1, p_2 be distinct odd primes and $k = p_1p_2$.
Let $n \equiv j\ (mod\ p_1p_2)$, where $j = 0, 1, 2, ..., \overline{p_1p_2 - 1}$. Then

$$|\bigcup_{j=0}^{p_1p_2-1} E_j^n| = (p_1^3 - 1)(p_2^3 - 1).$$

Proof. Since the congruence relation is an equivalence relations, all the congruent classes for $n \equiv j(mod\ p_1p_2)$, where $j = 0, 1, 2, ..., \overline{p_1p_2 - 1}$ define a partition. This means that there is an empty intersection between them.
Thus by Inclusion-Exclusion Principle, we have

$$|\bigcup_{j=0}^{p_1p_2-1} E_j^n| = \sum_{j=0}^{p_1p_2-1} |E_j^n|.$$

In view of Lemma 3.1, it is easy to see that there are 9 possible cases to find the number $|E_{p_1p_2}^n|$, where p_1 and p_2 are distinct odd primes. Since for any odd prime q there are $\frac{q-1}{2}$ square residues and $\frac{q-1}{2}$ are the square non-residues. Thus to find the sum of all cardinalities, we multiply each of the nine cardinalities by their weights as under:
(1) Multiply by $(\frac{p_1-1}{2})(\frac{p_2-1}{2})$ if $\left(\frac{j}{p_1p_2}\right) = \pm 1$ for all $j = 1, 2, ..., \overline{p_1p_2 - 1}$.
(2) Multiply by $(\frac{p_1-1}{2})$ or by $(\frac{p_2-1}{2})$ if $\left(\frac{j}{p_1}\right) = \pm 1$ or $\left(\frac{j}{p_2}\right) = \pm 1$ respectively for all $j = 1, 2, ..., \overline{p_1p_2 - 1}$.
(3) Multiply by integer 1 if none of (1) and (2) hold. Thus, $|\bigcup_{j=0}^{p_1p_2-1} E_j^n|$

$$\begin{aligned}
&= p_1p_2(p_1+1)(p_2+1)(\frac{p_1-1}{2})(\frac{p_2-1}{2}) + p_1p_2(p_1-1)(p_2-1)(\frac{p_1-1}{2})(\frac{p_2-1}{2})\\
&+ p_1p_2(p_1-1)(p_2+1)(\frac{p_1-1}{2})(\frac{p_2-1}{2}) + p_1p_2(p_1+1)(p_2-1)(\frac{p_1-1}{2})(\frac{p_2-1}{2})\\
&+ p_1(p_1-1)(p_2-1)(p_2+1)(\frac{p_1-1}{2}) + p_1(p_1+1)(p_2-1)(p_2+1)(\frac{p_1-1}{2})\\
&+ (p_1+1)(p_1-1)p_2(p_2+1)(\frac{p_2-1}{2}) + (p_1+1)(p_1-1)p_2(p_2-1)(\frac{p_2-1}{2})\\
&+ (p_1+1)(p_1-1)(p_2+1)(p_2-1)\\
&= (\frac{p_1p_2}{4})(p_1^2-1)(p_2^2-1) + (\frac{p_1p_2}{4})(p_1-1)^2(p_2-1)^2 + (\frac{p_1p_2}{4})(p_1-1)^2(p_2^2-1)\\
&+ (\frac{p_1p_2}{4})(p_1^2-1)(p_2-1)^2 + (\frac{p_1}{2})(p_1-1)^2(p_2^2-1) + (\frac{p_2}{2})(p_1^2-1)(p_2^2-1)\\
&+ (\frac{p_1}{2})(p_1^2-1)(p_2^2-1) + (\frac{p_2}{2})(p_1^2-1)(p_2-1)^2 + (p_1^2-1)(p_2^2-1)\\
&= (\frac{p_2}{2})(p_2^2-1)\{(\frac{p_1}{2})(p_1^2-1) + (\frac{p_1}{2})(p_1-1)^2 + (p_1^2-1)\} + (\frac{p_2}{2})(p_2-1)^2\{(\frac{p_1}{2})(p_1^2-1)\\
&+ (\frac{p_1}{2})(p_1-1)^2 + (p_1^2-1)\} + (p_2^2-1)\{(\frac{p_1}{2})(p_1^2-1) + (\frac{p_1}{2})(p_1-1)^2 + (p_1^2-1)\}\\
&= \{(\frac{p_1}{2})(p_1^2-1) + (\frac{p_1}{2})(p_1-1)^2 + (p_1^2-1)\}\{(\frac{p_2}{2})(p_2^2-1) + (\frac{p_2}{2})(p_2-1)^2 + (p_2^2-1)\\
&= (p_1^3-1)(p_2^3-1). \quad \square
\end{aligned}$$

Theorem 3.2. Let $p_1, p_2, ..., p_r$ be distinct odd primes and $g = \prod_{i=1}^{r} p_i^{k_i}$. Let ϕ denote the Euler-ϕ function. Then

$$|E_g^n| = \begin{cases} \phi(g^2)\prod_{i=1}^{r}(1+\frac{1}{p_i}) & \text{if } \prod_{i=1}^{r} p_i \mid n \\ \phi(g^2) & \text{if } \left(\frac{n}{p_i}\right) = -1 \text{ for all } i \\ g^2\prod_{i=1}^{r}(1+\frac{1}{p_i}) & \text{if } \left(\frac{n}{p_i}\right) = 1 \text{ for all } i \end{cases}$$

Proof. We apply induction on r. Let $r = 1$, then, $g = p_1^k$. For, if g divides n then p_1 divides n, Also

$$\begin{aligned} |E_g^n| &= \phi(p_1^{2k_1})(1+\frac{1}{p_1}) \\ &= \frac{(p_1^{2k_1} - p_1^{2k_1-1})(p_1+1)}{p_1} \\ &= p_1^{2(k_1-1)}(p_1^2-1). \end{aligned} \quad (1)$$

Next, we take $\left(\frac{n}{g}\right) = 1$. That is, $\left(\frac{n}{p_1^{k_1}}\right) = 1$. Then by Theorem 2.1, $\left(\frac{n}{p_1}\right) = 1$. Also

$$\begin{aligned} |E_g^n| &= g^2\prod_{i=1}^{r}(1+\frac{1}{p_i}) \\ &= \frac{p_1^{2k_1}(p_1+1)}{p_1} \\ &= p_1^{2(k_1-1)}p(p+1). \end{aligned} \quad (2)$$

Similarly, it can be seen that

$$|E_g^n| = \phi(g^2) = p_1^{2(k_1-1)}p(p-1), \left(\frac{n}{p_1}\right) = -1. \quad (3)$$

Hence by equations (1) to (3) and by Lemma 3.1, we see that our result is true for $r = 1$. Let $l = \prod_{i=1}^{r-1} p_i^{k_i}$ and suppose,

$$|E_l^n| = \begin{cases} \phi(l^2)\prod_{i=1}^{r-1}(1+\frac{1}{p_i}), & \text{if } l \mid n \\ \phi(l^2), & \left(\frac{n}{l}\right) = -1 \\ l^2\prod_{i=1}^{r-1}(1+\frac{1}{p_i}), & \left(\frac{n}{l}\right) = 1 \end{cases}$$

Take $g = lp_r^{k_r}$. Since $(l, p_r) = (\prod_{i=1}^{r-1} p_i, p_r) = 1$, hence by Theorem 2.2 and Lemma 3.1, we obtain,

$$\begin{aligned}
|E_g^n| &= |E_l^n||E_{p_r^{k_r}}^n| \\
&= \phi(l^2)\prod_{i=1}^{r-1}(1+\frac{1}{p_i})(p_r^{2(k_r-1)}(p_r^2-1)) \\
&= \phi(l^2)\prod_{i=1}^{r-1}(1+\frac{1}{p_i})(\phi(p_r^{2k_r})(1+\frac{1}{p_r}) \\
&= \phi(l^2p_r^{2k_r})\prod_{i=1}^{r}(1+\frac{1}{p_i}),\ \text{as } \phi(mn)=\phi(m).\phi(n),(m,n)=1 \\
&= \phi(g^2)\prod_{i=1}^{r}(1+\frac{1}{p_i}).
\end{aligned}$$

The rest of the cases can be proved in a similar technique. □

Corollary 3.1. Let $p_1, p_2, ..., p_r$ be distinct odd primes and σ denote the sum of positive divisors of $g=\prod_{i=1}^{r} p_i^{k_i}$. If $g \mid n$ then $|E_g^n| \leq \sigma(g)\phi(g)$.

Proof. Let $g=\prod_{i=1}^{r} p_i^{k_i}$, then it is easy to see that $0<\lfloor d(g)\rfloor \leq 1$ where,

$$d(g)=\prod_{i=1}^{r}\frac{p_i^{k_i-1}(p_i^2-1)}{p_i^{k_i+1}-1}.$$

For the proof of the above corollary, we first see that,

$$\begin{aligned}
\sigma(g)\phi(g)d(g) &= \prod_{i=1}^{r}\frac{p_i^{k_i+1}-1}{p_i-1}\prod_{i=1}^{r}(p_i^{k_i}-p_i^{k_i-1})\prod_{i=1}^{r}\frac{p_i^{k_i-1}(p_i^2-1)}{p_i^{k_i+1}-1} \\
&= \prod_{i=1}^{r}\frac{p_i^{k_i+1}-1}{p_i-1}(p_i^{k_i}-p_i^{k_i-1})\frac{p_i^{k_i-1}(p_i^2-1)}{p_i^{k_i+1}-1} \\
&= \phi(g^2)\prod_{i=1}^{r}(1+\frac{1}{p_i}) \\
&= |E_g^n|. \qquad (4)
\end{aligned}$$

But by the choice of $d(g)$, we have,

$$\sigma(g)\phi(g)d(g) \leq \sigma(g)\phi(g).$$

Hence, by (4), $|E_g^n| \leq \sigma(g)\phi(g)$. □

The following theorem is the generalization of Theorem 3.1 for an odd modulus.

Theorem 3.3. Let $p_1, p_2, ..., p_r$ be distinct odd primes and $g=\prod_{i=1}^{r} p_i^{k_i}$.
Let $n \equiv j\ (mod\ g)$, where, $j=0,1,2,...,\overline{g-1}$. Then

$$|\bigcup_{j=0}^{g-1} E_j^n| = g^3\prod_{i=1}^{r}(1-\frac{1}{p_i^3}).$$

Proof. We apply induction on r. Let $r=1$, then $g=p_1^{k_1}=p^k$(say). We know that amongst the $\phi(p^k)$ integers from Reduced Residue System (RRS) (mod p^k), half are quadratic residues and half are quadratic non-residues. So each of them is $\frac{1}{2}p^{k-1}(p-1)$ in numbering. Since there are p^k integers in Complete Residue system (CRS) (mod p^k), so $p^k-p^{k-1}(p-1)=p^{k-1}$ integers namely, $0, p, 2p, ..., p^{k-2}p$, are neither quadratic residue nor quadratic non residue of p^k. Then by Theorem 3.1, we obtain,

$$\begin{aligned}|\bigcup_{j=0}^{g-1} E_j^n| &= p^{k-1}\phi(p^{2k})(1+\frac{1}{p}) + \frac{p^{k-1}(p-1)}{2}p^{2k}(1+\frac{1}{p}) + \frac{p^{k-1}(p-1)}{2}\phi(p^{2k}) \\ &= p^{3k-3}(p^2-1) + \frac{1}{2}p^{3k-2}(p-1)^2 + \frac{1}{2}p^{3k-2}(p^2-1) \\ &= p^{3k-3}(p^2-1) + p^{3k-1}(p-1) \\ &= p^{3k-3}(p^3-1) \\ &= p^{3k}(1-\frac{1}{p^3}) \\ &= g^3(1-\frac{1}{p_1^3}). \qquad (5)\end{aligned}$$

Next we take $l = \prod_{i=1}^{r-1} p_i^{k_i}$ and we let,

$$|\bigcup_{j=0}^{l-1} E_j^n| = l^3 \prod_{i=1}^{r-1}(1-\frac{1}{p_i^3}). \qquad (6)$$

Write $g = lp_r^{k_r}$, where $l = \prod_{i=1}^{r-1} p_i^{k_i}$. Thus $(l, p_r^{k_r}) = 1$. Hence, by Theorem 2.2, we have,

$$|\bigcup_{j=0}^{g-1} E_j^n| = |\bigcup_{j=0}^{l-1} E_j^n||\bigcup_{j=0}^{p_r^{k_r}-1} E_{j=0}^n|. \qquad (7)$$

Substituting the values of (5) and (6) in (7), we get,

$$\begin{aligned}|\bigcup_{j=0}^{g-1} E_j^n| &= l^3 \prod_{i=1}^{r-1}(1-\frac{1}{p_i^3})p_r^{3k_r}(1-\frac{1}{p_r^3}) \\ &= g^3 \prod_{i=1}^{r}(1-\frac{1}{p_i^3}). \quad \square\end{aligned}$$

4. $G-$ Orbits of $Q^*(\sqrt{n})$

We propose algorithms to enumerate the $PSL(2,Z)$-orbits of $Q^*(\sqrt{n}\ )$. The notion of the algorithms is elaborated as follows.
We organize the elements of the infinite set $Q^*(\sqrt{n}\ )$ in term of finite classes of the form $[a,b,c]$ modulo n, where n is a non-square positive integer and $(a,b,c)=1$, provided $bc = a^2-n$. We use theorems given in Section 3, to find the classes for a given integer m. Recall that if $\alpha\bar{\alpha} < 0$, then α is called an ambiguous number. After finding the classes of the elements of $Q^*(\sqrt{n}\ )$, we use Algorithm 4.1, to find all ambiguous numbers related to classes for the given integer m. In Algorithm 4.2, we label a key to In function. This key will confirm whether a number selected in Algorithm 4.1, is an ambiguous number? A closed path under some element $(xy)^{n_1}(xy^2)^{n_2}...(xy)^{n_k}$ of the group G is called an orbit of G if the path is traversed from ambiguous to ambiguous (for detail see [6]). In Algorithm 4.3, we find $G-$orbits of $Q^*(\sqrt{n}\ )$ under the action of the modular group $PSL(2,Z)$ together with the mapping, the element of the G which fix the first vertex of that path. Finally, we use Algorithm 4.4 to find the length of that path or the ambiguous length.

4.1. Algorithm (Finding Ambiguous Numbers)

g: List of Classes
q: Number of Classes
j=o;

for $i = 0$ to $q - 1$ do
Alpha = $\frac{g[i].a+sqrt(n)}{g[i].c}$
Alpha Conjugate = $\frac{g[i].a-sqrt(n)}{g[i].c}$
If (Alpha * Alpha Conjugate < 0)
Ambiguous $[j++]$ = Alpha
end for

4.2. Algorithm (Ambiguous, Key)

In (Ambiguous, Key)
for $i = 0$ to Ambiguous.length-1
If key = = Ambiguous[i]
return true
else
return false
end for

4.3. Algorithm (Finding Mappings)

Array Map; $j = 0$
$k = 0$;
Initial Alpha = Alpha = Ambiguous [0]
do {
If ($k \ mod\ 2 == 0$)
$r = 0$;
{ do {
temp1 = Map$x(\alpha)$
temp2 = Map$y(\alpha)$
r = ++ }
while (! In (Ambiguous, temp1*temp2)
Map[j]= r
j++;
k++;
Alpha = temp1*temp2
}
else
{ $r = 0$ do
{ temp1 = Map$x(\alpha)$
temp2 = Map$y(\alpha)$
$r++$
}
while (! In (Ambiguous, temp1*temp2*temp2)
Alpha = temp1*temp2*temp2
Map[j]=r
j++;
k++; } }
while (Alpha ! In = initial Alpha)
return Map
}

4.4. Algorithm (Ambiguous length)

```
temp = 0
{ for i = 0 to Map.lenth−1
{ temp = temp + Map[i];
}
return temp
}
```

5. Conclusion

The intricacy of a typical method for finding orbits of an invariant set using projective special linear group, $PSL(2, Z)$ is based on coset diagram. This ordinary technique is seemed to be strenuous and laborious. In this piece of work we have suggested a novel technique that drastically reduces the complexity for the computations and enumeration of $G-$orbits, where G is $PSL(2, Z)$. Additionally the method developed is an explicit technique which does not require any sort of coset diagrams for finding orbits of $Q^*(\sqrt{n}\ )$ under G. Therefore, the technique developed in this paper perform much faster in contrast with existing techniques. Particularly, the cardinality of the the set E_g, consisting of all classes $[a, b, c]$ mod g, of the elements in $Q^*(\sqrt{n}\ )$ has been determined and shown to be equal to $g^3 \prod_{i=1}^{r}(1 - \frac{1}{p_i^3})$. The algorithm developed for the enumeration of orbits using classification of the elements in $Q^*(\sqrt{n}\ )$ efficiently validates the correctness of the formal technique discussed in this article. The numerical productions of the algorithm were coherent with the analytical findings.

REFERENCES

[1] *I.N. Herbert S. Zuckerman*, An introduction to the Theory of Numbers, John wiley & sons, Inc., 2005.

[2] *M. Aslam Malik and M. Asim Zafar*, Real Quadratic Irrational Numbers and Modular Group Action. Southeast Asian Bulletin of Mathematics, **35** (2011), No. 3, 439-445.

[3] *M. Aslam Malik and M. Asim Zafar*, G-subsets of an Invariant subset $Q^*(\sqrt{k^2m}\ )$ of $Q(\sqrt{m}\ ) \setminus Q$ Under the Modular Group Action, Utilitas Mathematica, **91** (2013), 377-387.

[4] *S. M. Husnine, M. Aslam Malik and A. Majeed*, On Ambiguous Numbers of an invariant subset $Q^*(\sqrt{k^2m})$ of $Q(\sqrt{m})$ under the action of the Modular Group PSL(2,Z). Studia Scientiarum Mathematicarum Hungarica, **42** (2005), No. 4, 401-412.

[5] *M. Aslam Malik and M. Khalid Mahmood*, Some Invariant Subsets of $Q^*(\sqrt{n}\ )$ Under the Action of $PSL(2, Z)$. International Mathematical Forum, **6** (2011), No. 32, 1557-1565.

[6] *Q. Mushtaq*, On word structure of the Modular Group over finite and real quadratic fields. Discrete Mathematics, **179** (1998), 145-154.

[7] *Shin-Ichi Katayama et al.*, Orbit of Quadratic Irrationals Modulo p by the Modular Group, Gomal University Journal of Research, **25** (2009), No. 1, 1-5.

[8] *G. Higman and Q. Mushtaq*, Coset Diagrams and Relations for PSL(2,Z). Gulf J.Sci. Res., **1** (1983), 159-164.

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