International Mathematical Forum, Vol. 7, 2012, no. 39, 1915 - 1924

A Classification of the Real Quadratic Irrational Numbers $\frac{a+\sqrt{n}}{c}$ of $Q^*(\sqrt{n})$ w.r.t Modulo 3^r

Farkhanda Afzal [1], Qamar Afzal and M. Aslam Malik

Department of Mathematics
University of the Punjab, Lahore, Pakistan
farkhanda_imran@live.com[1]

Abstract

This paper provides the classification of the Real Quadratic irrational numbers $\frac{a+\sqrt{n}}{c}$ of $Q^*(\sqrt{n})$ with respect to modulo 3^r. A general formula has been ascertained for this classification, by finding and subdividing the elements into the corresponding classes. Using this formula, we have calculated the cardinality of the set $I_{3^r}^{n}$ with n modulo 3^r.

Mathematics Subject Classification: 05C25, 11E04, 20G15

Keywords: Real Quadratic Irrational, Relatively Prime, Equivalence Classes, Complete Residue System

1- Introduction and Preliminaries

It was proved in [19] that every real quadratic irrational number can be written uniquely as $\frac{a+\sqrt{n}}{c}$, where n is a non-square positive integer and $a, \frac{a^2-n}{c}, and\ c$ are relatively prime integers.

Let $n = k^2m$, where m, a square free positive integer and k is non-zero integer. The set $Q^*(\sqrt{n}) = \left\{ \frac{a+\sqrt{n}}{c}; a, c \ \&\ b = \frac{a^2-n}{c} \text{ are integers } \&\ (a,b,c) = 1 \right\}$ is a subset of the real quadratic field $\mathrm{Q}(\sqrt{\mathrm{m}})$ for all k. A classification of the elements

$\frac{a+\sqrt{p}}{c}, b = \frac{a^2-p}{c}$ of $Q^*(\sqrt{p})$, where p is an odd prime with respect to odd even nature of a, b, c was discussed I Kausar [4].

Definition1.1: Let $[a, b, c](\text{mod } s)$ be the equivalence class of $\alpha = \frac{a+\sqrt{n}}{c}$ in $Q^*(\sqrt{n})$, and let I_S be the set of all such classes$[a, b, c](mods)$,For each value of $s > 1$, we get different equivalence classes of the form $[a, b, c]$ modulo s of $Q^*(\sqrt{n})$with $0 \leq a, b, c < s$ and $n$modulo s. that is $n \equiv i \pmod s$ for some $0 \leq i \leq s - 1$**.**

Definition 1.2: Let $s > 1$ be a fixed positive integer, for each $i \in \{0, 1, 2, \cdots, s - 1\}$. Let I_s^i(or I_s^n) be the set of all equivalence classes $[a, b, c](\text{mod } s)$ of the elements of $Q^*(\sqrt{n})$ with $n \equiv i \pmod s$. These classes partition the set I_s into disjoint sets of the form I_s^i for $0 \leq i \leq s - 1$ i.e. the union of these set is whole I_s and intersection is empty.

Theorem 1.1: If $r_1, r_2, r_3, \cdots, r_m$ is a complete residue module m, and if a is a positive integer with $(a, m) = 1$ then $ar_1 + b, ar_2 + b, ar_3 + b, \cdots, ar_m + b$ is a complete system of residue modulo m for any integer b. [7]

Definition 1.3: Let n be a fixed positive integer. Two integers a and b are said to be congruent modulo m, symbolized by $a \equiv b \pmod m$ if m divides the difference $a - b$ that is, provided that $a - b = km$ for some integer k[2]**.** M Aslam [11] generalized the concept of classification of elements of $Q^*(\sqrt{n})$ by using the idea of congruence.

Let $\alpha = \frac{a+\sqrt{n}}{c}$ where $b = \frac{a^2-n}{c}$ and $(a, b, c) = 1$ and s be a fixed positive integer. We say that α is of the form $[u, v, w]$ where u, v, w are the integers s.t $u \equiv a \pmod s$, $u \equiv b \pmod s$, and $w \equiv c \pmod s$. If $= \frac{a+\sqrt{n}}{c}$, $b = \frac{a^2-n}{c}$ and $\alpha' = \frac{a'+\sqrt{n}}{c'}$ where $b' = \frac{(a')^2-n}{c'}$ be two elements of $Q^*(\sqrt{n})$. We say that α and α' are of the same form if $a \equiv a' \pmod s$, $b \equiv b' \pmod s$ and $c \equiv c' \pmod s$.

2- A Classification of the elements of $Q^*(\sqrt{n})$ with respect to modulo 3^r

These equivalence classes play a vital role in the formation of G and M subsets of $Q(\sqrt{m})$. It is also a very useful technique to calculate the orbits of certain invariant subsets of real quadratic fields under the action of Mobius groups. To comprehend the significance of these congruence classes, it has become a requisite to generalize the classification of elements of $Q^*(\sqrt{n})$ with respect to prime power moduli. In this regard we started for first odd prime3 and investigated the classification of elements of $Q^*(\sqrt{n})$ in modulo 3^rin this paper.

Definition 2.1: We define $I_{3^r}^n$; $r \in Z^+$ to be the set of all classes $[a, b, c]$ modulo 3^r of the elements of $Q^*(\sqrt{n}) = \left\{ \frac{a+\sqrt{n}}{c};\ a, b = \frac{a^2-n}{c}, c \in Z; (a, b, c) = 1 \right\}$; $n \equiv 0, 1, 2, \cdots,$ or $3^r - 1 \pmod{3^r}$. The following theorem is concerned with the cardinality of $I_{3^r}^n$ for each $n \equiv 0, 1$ or $2 \pmod 3$

Theorem 2.1: $|I_3^n| = \begin{cases} 08 & \text{if } n \equiv 0 \pmod 3 \\ 12 & \text{if } n \equiv 1 \pmod 3 \\ 06 & \text{if } n \equiv 2 \pmod 3 \end{cases}$ [11]

Proof: Let $\frac{a+\sqrt{n}}{c} \in Q^*(\sqrt{n})$. Thus we know that $(a, b, c) = 1$, so all a, b, c cannot be $\equiv 0\ (mod\ 3)$, since $n \equiv 0, 1\ or\ 2\ (mod\ 3)$. Thus we have three cases for three possible values of n. We discuss each of these separately.

Case I:

i- Let $n \equiv 0 \pmod 3$ and $a \equiv 0 \pmod 3$, then $a^2 - n \equiv 0\ (mod\ 3)$. Therefore exactly one of b, c is $\equiv 0\ (mod\ 3)$ and other is either $\equiv 1\ (mod\ 3)$ or $\equiv 2\ (mod\ 3)$

ii- When $n \equiv 1\ or\ 2\ (mod\ 3)$, then $a^2 - n \equiv 1\ (mod\ 3)$. So both of b and c are either $\equiv 1\ (mod\ 3)$ *or* $\equiv 2\ (mod\ 3)$.

Thus for $n \equiv 0 \pmod 3$, then there are 8 equivalence classes of elements of $Q^*(\sqrt{n})$ of the forms [0, 0, 1], [0, 0, 2], [0, 1, 0], [0, 2, 0], [1, 1, 1], [1, 2, 2], [2, 1, 1] and [2, 2, 2]

Case II: when $a \equiv 1 \pmod 3$,

i- If $a \equiv 0 \pmod 3 \Longrightarrow a^2 - n \equiv 2 \pmod 3$. Hence exactly one of th $b, c \equiv 2 \pmod 3$ and other is $\equiv 1 \pmod 3$

ii- If $a \equiv 1$ or $2 \pmod 3 \Longrightarrow a^2 - n \equiv 0 \pmod 3$. Therefore at least one of $b, c \equiv 0\ (mod\ 3)$ and other may be $\equiv 0, 1\ or\ 2\ (mod\ 3)$.

Thus the 12 equivalence classes of $Q^*(\sqrt{n})$ for $n \equiv 1\ (mod\ 3)$ are of forms [0, 2, 1], [0, 1, 2], [1, 0, 1], [1, 1, 0], [1, 0, 2], [1, 2, 0], [2, 0, 1], [2, 1, 0], [2, 0, 2], [2, 2, 0], [2, 0, 0] and [1, 0, 0].

Case III: when $a \equiv 2 \pmod 3$,

i- For the case when $a \equiv 0 \pmod 3 \Longrightarrow a^2 - n \equiv 1 \pmod 3$.Hence both b, c are either $\equiv 1\ (mod\ 3)$ *or* $\equiv 2(mod\ 3)$.

ii- when $a \equiv 1\ or\ 2\ (mod\ 3) \Longrightarrow a^2 - n \equiv 2\ (mod\ 3)$. Hence one of b, c *is* $\equiv 2\ (mod\ 3)$ and other is $\equiv 1 \pmod 3$.

Therefore [0, 1, 1], [0, 2, 2], [1, 1, 2], [1, 2, 1], [2, 2, 1], and [2, 1, 2] are exactly six forms of classes of $Q^*(\sqrt{n})$ when $a \equiv 2 \pmod 3$.

Hence $\left|I_{3^1}^n\right| = \begin{cases} 08 & \text{if } n \equiv 0 \pmod 3 \\ 12 & \text{if } n \equiv 1 \pmod 3 \\ 06 & \text{if } n \equiv 2 \pmod 3. \end{cases}$

Theorem 2.2: Let $r \geq 1$ be a fixed integer and let $[\ a_r',\ b_r',\ c_r'\ ] \pmod{3^r}$ be an equivalence class of $Q^*(\sqrt{n})$ with $n \equiv n_r' \pmod{3^r}$, then $[\ a_r' + a_r \cdot 3^r, 0 b_r' + b_r \cdot 3^r, 0\ c_r' + c_r \cdot 3^r\ ] \pmod{3^{r+1}}$with a_r, b_r, c_r are fixed and $a_r, b_r, c_r \in F_3 = \{0, 1, 2\}$ be an equivalence class of $Q^*(\sqrt{n})$, where $n \equiv (a_r')^2 - b_r' c_r' + k\ 3^r \pmod{3^{r+1}}$ with a unique integer of $k, 0 \leq k < 3$ given by $k \equiv 2[\ a_r' a_r + b_r' c_r + b_r' c_r] \pmod 3$

Proof: Since we can represent $a, b,$ and c in base 3 as$a = a_0 + a_1 \cdot 3 + \cdots + a_{r-1} \cdot 3^{r-1} + a_r \cdot 3^r$, $b = b_0 + b_1 \cdot 3 + \cdots + b_{r-1} \cdot 3^{r-1} + b_r \cdot 3^r$ and $c = c_0 + c_1 \cdot 3 + \cdots + c_{r-1} \cdot 3^{r-1} + c_r \cdot 3^r$; $a_r, b_r, c_r \in F_3 = \{\ 0, 1, 2\ \}$. Then we can write $a = a_r' + a_r 3^r$, $b = b_r' + b_r 3^r$ and $c = c_r' + c_r 3^r$, where $a_r' = a_0 + a_1 \cdot 3^r + \cdots + a_{r-1} \cdot 3^{r-1}$, $b_r' = b_0 + b_1 \cdot 3^r + \cdots + b_{r-1} \cdot 3^{r-1}$ and $c_r' = c_0 + c_1 \cdot 3^r + \cdots + c_{r-1} \cdot 3^{r-1}$.Let $[\ a_r',\ b_r',\ c_r'\ ] \pmod{3^r}$ be any class of $Q^*(\sqrt{n})$ with $n \equiv n_r' \pmod{3^r}$, then $(a_r')^2 - b_r' c_r' \equiv n_r' \pmod{3^r}$.

We have to prove that $a^2 - bc \equiv (a_r')^2 - b_r'c_r' + k\,3^r \pmod{3^{r+1}}$ with a unique integer k such that $k \equiv 2[\,a_r' a_r + b_r' c_r + b_r c_r'\,] \pmod 3$. Suppose $f(x) = (a_r')^2 - b_r' c_r' + [\,2a_r' a_r - b_r' c_r - b_r c_r'\,]\,3^r + [\,a_r^2 - b_r c_r\,]\,3^{2r} - x$ ..... **(1)**
Then $f'(x) = -1$ ..... **(2)**. $f((a_r')^2 - b_r'c_r') = (a_r')^2 - b_r' c_r' + [\,2a_r' a_r - b_r' c_r - b_r c_r'\,]\,3^r + [\,a_r^2 - b_r c_r\,]\,3^{2r} - (a_r')^2 - b_r'c_r'$. Thus $f((a_r')^2 - b_r'c_r') \equiv 0 \pmod{3^r}$. Also by Equation (2) $f'((a_r')^2 - b_r'c_r') \not\equiv 0 \pmod 3$. Hence by **Hensel's Lemma** there exists $k, 0 \le k < 3$, such that $f((a_r')^2 - b_r'c_r' + k\,3^r) \equiv 0 \pmod{3^{r+1}}$ where k is given by

$$\begin{aligned} k &\equiv -\frac{\overline{f'\left((a_r')^2 - b_r'c_r'\right)}}{3^r} f((a_r')^2 - b_r'c_r') \pmod 3 \\ &\equiv (2a_r' a_r - b_r' c_r - b_r c_r') \pmod 3. \\ &\equiv 2[\,a_r' a_r + b_r' c_r + b_r c_r'\,] \pmod 3 \end{aligned}$$

Where $\overline{f'((a_r')^2 - b_r'c_r')}$ is the multiplicative (conjugate) inverse of $f'((a_r')^2 - b_r'c_r') \pmod 3$, i.e., by (1) $(a_r')^2 - b_r' c_r' + [2a_r' a_r - b_r' c_r - b_r c_r'\,]\,3^r + [\,a_r^2 - b_r c_r\,]\,3^{2r} - ((a_r')^2 - b_r'c_r') - k3^r \equiv 0 \pmod{3^{r+1}}$.This implies:

$a^2 - bc - ((a_r')^2 - b_r' c_r') - k\,3^r \equiv 0 \pmod{3^{r+1}}$, then $a^2 - bc \equiv (a_r')^2 - b_r' c_r' + k\,3^r \pmod{3^{r+1}}$ where $k \equiv 2[a_r'a_r + b_r'c_r + b_r'c_r] \pmod 3$.

Corollary2.1:
Let $(a_r')^2 - b_r'c_r' \equiv n_r' \pmod{3^r}$,Then $n \equiv (n_r' + n_r 3^r) \pmod{3^{r+1}}$.
Proof: Suppose $(a_r')^2 - b_r'c_r' \equiv n_r' \pmod{3^r}$, then by Definition 1.3, we have $(a_r')^2 - b_r'c_r' = n_r' + k'3^r$ for some $k' \in Z$. Also from Theorem 2, we get

$$\begin{aligned} n &\equiv [(a_r')^2 - b_r'c_r' + k'3^r] \pmod{3^{r+1}} \\ &\equiv [n_r' + k \cdot 3^r + k' \cdot 3^r] \pmod{3^{r+1}} \\ &\equiv [n_r' + (k + k')\,3^r] \pmod{3^{r+1}};\ k \in z \text{ and } k' \in \{0,1,2\} \end{aligned}$$

$\Longrightarrow n \equiv (n_r' + n_r 3^r) \pmod{3^{r+1}}$, where $n_r = k + k' \in \{0,1,2\}$. As $k' \in \{0,1,2\}$ which is a complete residue system modulo 3. If k is any integer then $k + k'$ is also a complete residue system of modulo 3 by Theorem 1.1. Hence $n \equiv (n_r' + n_r 3^r) \pmod{3^{r+1}};\ n_r \in \{0,1,2\}$, this completes the proof.

Corollary 2.2: From Theorem 2.2 and Corollary 2.1, we have $n_r \equiv 2[a_r'a_r + b_r'c_r + b_r'c_r] \pmod 3$ In particular if $a_r, b_r, c_r \in F_3 = \{0, 1, 2\}$, then $[\,a_r' + a_r \cdot 3^r, 0b_r' + b_r \cdot 3^r, 0\,c_r' + c_r \cdot 3^r\,] \pmod{3^{r+1}}$ have 27 possible forms with n_r $0, 1$ or $2 \pmod 3$ exactly 9 times each.

Proof: In particular if $a_r, b_r, c_r \in F_3 = \{0, 1, 2\}$ then we prove that the 27 possible forms $[\, a'_r + a_r \cdot 3^r, 0 b'_r + b_r \cdot 3^r, 0\ c'_r + c_r \cdot 3^r\ ] \pmod{3^{r+1}}$of elements $Q^*\left(\sqrt{n}\,\right)$, where $n \equiv n'_r + n_r \cdot 3^r \pmod{3^{r+1}}$ with $n_r = 0,1$ or 2 equal number of times. Thus by putting all the values of a_r, b_r, c_r and arranging these also, we get 27 combinations of n_r in modulo 3

[Throughout this section we take the following 27 combinations of n_r (consisting of 9 sets of equations) as 27 combinations of type $(*)$].

$$\underbrace{0,\ a'_r,\ 2a'_r}\ ;\ \underbrace{b'_r,\ a'_r + b'_r,\ 2a'_r + b'_r}\ ;$$
$$\underbrace{c'_r,\ a'_r + c'_r,\ 2a'_r + c'_r}\ ;\ \underbrace{2b'_r,\ a'_r + 2b'_r,\ 2a'_r + 2b'_r}\ \underbrace{2c'_r,\ a'_r + 2c'_r,\ 2a'_r + 2c'_r}\ ;$$
$$\underbrace{2(b'_r + c'_r),\ a'_r + 2(b'_r + c'_r),\ 2a'_r + 2(b'_r + c'_r)};$$
$$\underbrace{(b'_r + c'_r),\ a'_r + (b'_r + c'_r),\ 2a'_r + (b'_r + c'_r)};$$
$$\underbrace{(2b'_r + c'_r),\ a'_r + (2b'_r + c'_r),\ 2a'_r + (2b'_r + c'_r}\ ;$$
$$\underbrace{(b'_r + c'_r),\ a'_r + (b'_r + c'_r),\ 2a'_r + (b'_r + c'_r)}. \qquad (*)$$

By Theorem 2.1, we know that the class $[a'_r,\ b'_r,\ c'_r] \pmod{3^r}$ has 26 (elements) possible forms $[a'_r,\ b'_r,\ c'_r]$ in modulo 3. So we discuss all these cases separately. It is important to note that $a'_r \equiv a_0 \pmod 3$, $b'_r \equiv b_0 \pmod 3$, $c'_r \equiv c_0 \pmod 3$ as $a'_r = a_0 + a_1 \cdot 3^r + \cdots + a_{r-1} \cdot 3^{r-1}$, $b'_r = b_0 + b_1 \cdot 3^r + \cdots + b_{r-1} \cdot 3^{r-1}$ and $c'_r = c_0 + c_1 \cdot 3^r + \cdots + c_{r-1} \cdot 3^{r-1}$.

Case I: When any two of $a_0, b_0,\ c_0$ are $\equiv 0 \pmod 3$. Say $a_0 \equiv 0 \pmod 3, b_0 \equiv 0 \pmod 3$ then $c_0 \not\equiv 0 \pmod 3$. The expression (*) yields:

$$\underbrace{0,\ 0,\ 0}\ ;\ \underbrace{0,\ 0,\ 0}\ ;\ \underbrace{c_0,\ c_0,\ c_0}\ ;\ \underbrace{2c_0,\ 2c_0,\ 2c_0}\ ;\ \underbrace{0,\ 0,\ 0};\ \underbrace{2c_0,\ 2c_0,\ 2c_0}\ ;$$
$$\underbrace{c_0,\ c_0,\ c_0}\ ;\ \underbrace{c_0,\ c_0,\ c_0}\ ;\ \underbrace{2c_0,\ 2c_0,\ 2c_0}\ .$$

As $c_0 \not\equiv 0 \pmod 3$ so $c_0 \equiv 1$ or $2 \pmod 3$, thus clearly $n_r = 0, 1$ or 2 and moreover out of these 27 values n_r, appears equal to 0, 1 or 2 exactly nine times each.

Case II**:** When only one of $a_0,\ b_0$ and $c_0 \equiv 0 \pmod 3$. We suppose without loss of generality that $a_0 \equiv 0 \pmod 3$ and $b_0 \not\equiv 0 \pmod 3$ and $c_0 \not\equiv 0 \pmod 3$. Then by 27 combinations of the types (*) takes forms:

$\underbrace{0,\ 0,\ 0}$; $\underbrace{b_0,\ b_0,\ b_0}$; $\underbrace{c_0,\ c_0,\ c_0}$; $\underbrace{2b_0,\ 2b_0,\ 2b_0}$;
$\underbrace{2b_0 + c_0,\ 2b_0 + c_0,\ 2b_0 + c_0}$;
$\underbrace{(b_0 + 2c_0), (b_0 + 2c_0),\ \ (b_0 + 2c_0)}$. ; $\underbrace{2c_0,\ 2c_0,\ 2c_0}$
; $\underbrace{2(b_0 + c_0),\ 2(b_0 + c_0),\ 2(b_0 + c_0)}$; $\underbrace{(b_0 + c_0), (b_0 + c_0),\ \ (b_0 + c_0)}$.

Now b_0, c_0 are either both $\equiv 1$ or $2 \pmod 3$ or one of them is $\equiv 1 \pmod 3$ and the other is $\equiv 2 \pmod 3$. And clearly in each of these cases the result holds again.

Case III**:** When at least one of $a_0, b_0,\ c_0$ are $\equiv 1 \pmod 3$ say $a_0 \equiv 1 \pmod 3$. Therefore remaining two b_0 and c_0 are either $\equiv 1 \pmod 3$ or $\equiv 2 \pmod 3$.Thus by 27 combinations of the types (*) we have:

$\underbrace{0,\ 0,\ 0}$; $\underbrace{b_0,\ 1 + b_0,\ 2 + b_0}$; $\underbrace{c_0,\ 1 + c_0,\ 2 + c_0}$; $\underbrace{2b_0,\ 1 + 2b_0,\ 2 + 2b_0}$;
$\underbrace{2c_0,\ 1 + 2c_0,\ 2 + 2c_0}$; $\underbrace{2(b_0 + c_0), 1 + 2(b_0 + c_0),\ 2 + 2(b_0 + c_0)}$;
$\underbrace{2b_0,\ 1 + 2b_0,\ 2 + 2b_0}$; $\underbrace{2c_0,\ 1 + 2c_0,\ 2 + 2c_0}$;
$\underbrace{(b_0 + c_0), 1 + (b_0 + c_0),\ \ 2 + (b_0 + c_0)}$.

Case IV**:** When all of $a_0,\ b_0, c_0$ are $\equiv 2 \pmod 3$, Then we have by 27 combinations of the types (*):

$\underbrace{0,\ 2,\ 1}$; $\underbrace{2,\ 1,\ 0}$; $\underbrace{2,\ 1,\ 0}$; $\underbrace{1,\ 0,\ 2}$; $\underbrace{1,\ 0,\ 2}$; $\underbrace{2,\ 1,\ 0}$; $\underbrace{1,\ 0,\ 2}$;
$\underbrace{0,\ 2,\ 1}$; $\underbrace{0,\ 2,\ 1}$

So we obtain apparently exactly 9 times each of 0, 1 and 2. Thus we prove that the 27 possible forms$[\ a'_r + a_r \cdot 3^r, 0b'_r + b_r \cdot 3^r, 0\ c'_r + c_r \cdot 3^r\ ] \pmod{3^{r+1}}$ of elements $Q^*(\sqrt{n}),\ n_r = 0,1$ or 2 equal number of times in all cases.

3- Cardinality of the set $\mathbf{I_{3^r}^n}$

We are now in a position to give a general formula for the cardinality of the set $I_{3^r}^n \equiv \{\,[a, b, c] \pmod 3 : \frac{a+\sqrt{n}}{c} \in Q^*(\sqrt{n})\}$ of the elements of $Q^*(\sqrt{n})$ with modulo 3^r.

Theorem 3.1 Let $r \geq 1$ be any integer, then

$$\left|I_{3^r}^n\right| = \begin{cases} 8 \text{ x } 9^{r-1} & \text{if } n \equiv 0 \pmod 3 \\ 12 \text{ x } 9^{r-1} & \text{if } n \equiv 1 \pmod 3 \\ 6 \text{ x } 9^{r-1} & \text{if } n \equiv 2 \pmod 3. \end{cases}$$

Proof: We prove this result by induction on r.

Step 1: For $r = 1$, the result holds from Theorem 2.1.

That is $\left|I_{3^1}^n\right| = \begin{cases} 8 & \text{if } n \equiv 0 \pmod 3 \\ 12 & \text{if } n \equiv 1 \pmod 3 \\ 6 & \text{if } n \equiv 2 \pmod 3. \end{cases}$

We know by the proof of Theorem 2.2, each $[a_0,\ b_0,\ c_0] \pmod 3$ of $Q^*(\sqrt{n})$ with $n \equiv n_0 \pmod 3$ gives exactly 27 classes of the forms $[a_0 + a_1 3,\ b_0 + b_1 3,\ c_0 + b_1 3\ ] \pmod{3^2}$ where $a_1,\ b_1,\ c_1 \in \{0,1,2\}$ such that $n \equiv n_0 + n_1 3^1 \pmod{3^2}$……(**1**) with $n_1 \equiv [a_0 a_1 + b_0 c_1 + c_0 b_1] \pmod 3$. Also by the Corollary 2.1 the possible values of n_1 are 0, 1 or 2 exactly 9 times each. Thus Congruence becomes $n \equiv n_0, l\, n_0 + 3$ or $n_0 + 2 \cdot 3 \pmod{3^2}$. accordingly as $n_1 = 0, 1$ or 2. Therefore,

$\left|I_{3^2}^n\right| = \begin{cases} 8 \text{ x } 9 & \text{if } n \equiv 0 \pmod 3 \\ 12 \text{ x } 9 & \text{if } n \equiv 1 \pmod 3 \\ 6 \text{ x } 9 & \text{if } n \equiv 2 \pmod 3. \end{cases}$. Hence the result holds for $r = 2$ also.

Step 2**:** Suppose that the result is true for $r = k$, i.e.,

$$\left|I_{3^k}^n\right| = \begin{cases} 8 \text{ x } 9^{k-1} & \text{if } n \equiv 0 \pmod 3 \\ 12 \text{ x } 9^{k-1} & \text{if } n \equiv 1 \pmod 3 \\ 6 \text{ x } 9^{k-1} & \text{if } n \equiv 2 \pmod 3. \end{cases}$$

Step 3**:** We show that the result holds for $r = k + 1$. From step 2, each $[a_k',\ b_k',\ c_k'] \pmod{3^k}$ is a class of $Q^*(\sqrt{n})$ modulo 3^k with $(a_k')^2 - b_k' c_k' \equiv n_k' \pmod{3^{k+1}}$. Again by Theorem 2.2, each $[a_k',\ b_k',\ c_k'] \pmod{3^k}$ gives 27 classes of forms $[a_k' + a_k 3^k, b_k' + b_k 3^k, c_k' + c_k 3^k] \pmod{3^{k+1}}$, where $n \equiv n_k',\ n_k' + 3^k, n_k' + n_k + 2 \cdot 3^k \pmod{3^{k+1}}$. Thus each class gives 9 times classes in raising power of moduli from 3^k to 3^{k+1} by Corollary 2.2. Therefore we have:

$$\left|I^n_{3^{k+1}}\right| = \begin{cases} 8 \text{ x } 9^k & \text{if } n \equiv 0 \pmod 3 \\ 12 \text{ x } 9^k & \text{if } n \equiv 1 \pmod 3. \\ 6 \text{ x } 9^k & \text{if } n \equiv 2 \pmod 3. \end{cases}$$

Thus the results hold for $r = k + 1$. Hence it holds for all $r \geq 1$.

References

[1] A. Adler and J.E Coury, The Theory of Numbers, by Jones and Barlett Publishers, 1995.

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

[3] G. Higman and Q. Mushtaq, Coset Diagrams and Relations for PSL (2, Z), Arab Gulf J. Sc, (1983), Res. 1 (1), pp 159-164.

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

[5] I.N. Herstein, Topics in Algebra, by John Wiley & Sons, Inc. 1975.

[6] J.S. Rose, A Course on Group Theory, by Dover Publications, Inc. New York. 1994.

[7] K.H Rosen, Elementary Number Theory and its Applications, by AT&T Laboratories, 2005.

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

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

[10] M. Aslam Malik, S.M. Husnine and A. Majeed, The orbits of $Q^*(\sqrt{p})$,$p = 2$ or $p \equiv 1 \pmod 4$ under the action of the Modular Group, PUJM, (2000), Vol. 33,pp 37-50.

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

[12] M.Aslam Malik, S.M. Husnine and A. 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, (2005), Vol. 42(4), pp 371-386.

[13] M. Aslam Malik, M. Asim Zafar, Real Quadratic Irrational Numbers and Modular group Action, Southeast Asian bulletin of Mathematics Vol. 35 (3) 2011, 439-445

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

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

[16] Q. Mushtaq, Modular Group Acting on Real Quadratic Fields, Bull Austral, Math, Soc. (1988), Vol. 37, pp303-309.

[17] Q. Mushtaq, On word structure of the Modular Group over finite and real quadratic fields, Discrete Mathematics (1998), 178, pp155-164.

[18] Q. Mushtaq and F. Shaheen, Cost Diagrams for a Homomorphic Image of $\Delta(2,3,6)$ ARS. Combinatoria (1987), 23A, pp 187-193.

[19] Q. Mushtaq and M. Aslam, Group Generated by two elements of orders 2 and 4 acting on real quadratic fields, Acta Mathematica Sinica, New Series, (1993), Vol.9, No.1, pp221-224

[20] Q. Mushtaq and M. Aslam, Group Generated by Two Elements of Orders Two and six acting on R and $Q(\sqrt{n})$, Discrete Mathematics (1998),179, pp145-154.

Received: March, 2012