Hindawi
Journal of Function Spaces
Volume 2022, Article ID 6320243, 11 pages
https://doi.org/10.1155/2022/6320243

Research Article

Mobius Group Generated by Two Elements of Order 2, 4, and Reduced Quadratic Irrational Numbers

Dilshad Alghazzawi,[1] **M. Haris Mateen**,[2] **M. Aslam Malik**,[3] **P. Hammachukiattikul**,[4] **and Mohammed S. Abdo**[5]

[1]*Department of Mathematics, King Abdulaziz University (Rabigh), Saudi Arabia*
[2]*Department of Management Science, National University of Modern Languages, Lahore, Pakistan*
[3]*Department of Mathematics, University of Punjab Lahore, 54590, Pakistan*
[4]*Department of Mathematics, Phuket Rajabhat University, Phuket 83000, Thailand*
[5]*Department of Mathematics, Hodeidah University, Al-Hudaydah, P.O. Box 3114, Yemen*

Correspondence should be addressed to P. Hammachukiattikul; porpattama@pkru.ac.th
and Mohammed S. Abdo; msabdo@hoduniv.net.ye

Received 9 December 2021; Accepted 14 March 2022; Published 7 April 2022

Academic Editor: Sarfraz Nawaz Malik

The construction of circuits for the evolution of orbits and reduced quadratic irrational numbers under the action of Mobius groups have many applications like in construction of substitution box (s-box), strong-substitution box (s.s-box), image processing, data encryption, in interest for security experts, and other fields of sciences. In this paper, we investigate the behavior of reduced quadratic irrational numbers (RQINs) in the coset diagrams of the set $Q''(\sqrt{m}) = \{\eta/s : \eta \in Q^*(\sqrt{m}), s = 1, 2\}$ under the action of group $H = <x', y' : x'^2 = y'^4 = 1>$, where m is square free integer and $Q^*(\sqrt{m}) = \{(a' + \sqrt{m})/c', (a', (a'^2 - m)/c'c') = 1, c' \neq 0\}$. We discuss the type and reduced cardinality of the orbit $Q''(\sqrt{p})$. By using the notion of congruence, we give the general form of reduced numbers (RNs) in particular orbits under certain conditions on prime p. Further, we classify that for a reduced number r whether $-r, \bar{r}, -\bar{r}$ lying in orbit or not. AMS Mathematics subject classification (2010): 05C25, 20G401.

1. Introduction and Preliminaries

Groups are very helpful algebraic structures, carrying other algebraic structures on them. In abstract algebra, almost all typical structures are illustration of groups. The significance of groups was derived from their action on special structures or spaces. Cryptography is the technique of converting secret knowledge into information and a type of data pretending to reach its terminus without leaking data safely. Modern cryptography is classified into several branches. Although there are two main research fields such that symmetric and public key cryptography, the public and private keys are used in public key cryptography. The same keys are used at both ends to encrypt and decrypt data/information in symmetric key cryptography. It is well known that the substitution box is a standout in symmetric key cryptography. Shahzad et al. investigated the efficient technique for the construction of an S-box by using action of a $PSL(2, Z)$. For constructing an S box, the vertices of the coset diagram are considered in a special way. In this way, the generated S box is highly safe and also closely meeting the optimal values of the standard S-box. In [1–6], the construction of substitution boxes based on coset graphs under the action of modular group $PSL(2, Z)$ has been discussed. In this piece of work, we investigate the structure of coset graphs under the action of modular group H. This work will be more helpful for construction of strong substitution boxes.

The H-circuits of the set upon which the groups act are the equivalence classes of group action. Group H can be

written in the form of relations and generators as $<x', y' : x'^2 = y'^4 = 1>$.

Assume that m is nonsquare integer, then $Q(\sqrt{m}) = \{s + t\sqrt{m} : s, t \in Q\}$. In 1878, Cayley was the first who introduced the technique of analysis of the groups through graphs. To investigate the action of infinite groups generated by finite elements on the infinite field by the coset diagram was first introduced by Higman in 1978. A number $\beta = s + t\sqrt{m} \in Q(\sqrt{m})$ is said to be ambiguous number (AN) if β and $\bar{\beta}$ have opposite signs. If $\beta = s + t\sqrt{m}$ is not ambiguous, then it is either totally positive or negative. The real quadratic irrational (RQI) numbers of the form $(a' + \sqrt{m})/c'$, where $(a', (a'^2 - m)/c', c') = 1$ and c' is nonzero integer, make the set represented as $Q^*(\sqrt{m})$. A RQI number $\beta = (a' + \sqrt{m})/c'$ is known as RQIN if $\beta > 0$ and $-1 < \bar{\beta} < 0$. In this paper, we will denote the reduced number by r. If there are k reduced numbers, then they are denoted by $r_1, r_2, r_3, \cdots r_k$. For $\beta \in Q''(\sqrt{m})$, in the orbit of $(\beta)^H$, the count of RQINs is called the reduced length (RL), which is denoted by $|(\beta)^H|_{\text{red}}$. These numbers are very less in $Q''(\sqrt{m})$ and play a significant part in the circuit of an orbit. A circuit made of vertices of a square and edges existing in H-orbits of $Q''(\sqrt{m})$, under the Mobius group H in coset diagram. If $((p_1)_0, (q_1)_1, (r_1)_2, (p_2)_0, (q_2)_1, (r_2)_2 \cdots (p_k)_0, (q_k)_1, (r_k)_2)$ is the type of a circuit, then it makes an element of group $h = (x'y')^{p_1}, (x'y'^2)^{q_1}, (x'y'^3)^{r_1}, (x'y')^{p_2}, (x'y'^2)^{q_2}, (x'y'^3)^{r_2}, \cdots (x'y')^{p_k}, (x'y'^2)^{q_k}, (x'y'^3)^{r_k}$ of H. This h fixes some element exists in this circuit.

In [7, 8], Mushtaq and Aslam presented that there are only finite number of ambiguous numbers (ANS); in the coset diagram for the orbit of $(\beta)^H$, the ambiguous numbers form unique closed path. A cost diagram is introduced in [7, 8] to investigate the action of an infinite group H on the projective line over real quadratic field (RQF). Malik and Zafar [9] investigated the properties of RQI numbers under the action of H. Zafar and Malik [10, 11] investigated the type and ambiguous lengths of the orbit of $Q''(\sqrt{p})$. Farkhanda and Qamar discussed the real quadratic irrational and action of $M = <x', y' : x'^2 = y'^6 = 1>$. Razaq et al. [12, 13] investigated the circuits of length 4 in $\text{PSL}(2, Z)$, group theoretic construction of highly nonlinear substitution box, and its applications in image encryption. Ali and Malik [14, 15] discussed the classification of $\text{PSL}(2, Z)$-circuits and investigated the RQIN and types of G-circuits with length four and six. Chen et al. [16] investigate reduced numbers which play an important role in the study of modular group action on the $PSL(2, Z)$-subset. For more studies of group action on various field, we recommend reading of [17, 18]. The application of group theory and group action is obvious to encryption, physics, and mechanics to construct models and their structures [5, 19–21]. Mateen et al. [22–27] investigated the structure of power digraphs associated with the congruence $x^n \equiv y (\text{mod } m)$, the partitioning of a set into two or more disjoint subsets of equal sums, and the symmetry of complete graphs and, moreover, investigated the importance of power digraphs in computer science. Alolaiyan et al. [28] discussed the homomorphic copies in coset graphs for the modular group.

The major contributions of this paper are given below.

(1) This paper presents a graphical study of the action of a Mobius group H on the real quadratic field (RQF)

(2) We discuss the classification of H-circuits and find the numbers that play vital role in the structure of H-circuits

(3) We investigate the RQINs and the types of H-circuits with different length

(4) We give the number of reduced numbers and their general form in different orbits for different values of p under a certain condition on p by using the concept of congruences

Theorem 1. [29]. *If $<b_1, b_2, b_2, \cdots, b_k>$ is symmetric continued fraction (CF) and $<b_1, b_2, b_2, \cdots, b_k> = (R + \sqrt{M})/s$, then $M = R^2 + S^2$.*

Theorem 2. [9]. *The set $\mathbb{Q}''(\sqrt{m}) = \{\eta/s : \eta \in \mathbb{Q}^*(\sqrt{m}), s = 1, 2\}$ is unchanged under the action of H.*

Theorem 3. [10]. *Let $m \equiv 1 (\text{mod } 8)$. Then, $\mathbb{Q}''(\sqrt{m})$ splits into four H-subsets. In particular, $(\sqrt{m}/1)^H$, $(\sqrt{m}/-1)^H$, $((1 + \sqrt{m})/2)^H$, and $((1 + \sqrt{m})/4)^H$ are at least four H-orbits of $\mathbb{Q}''(\sqrt{m})$.*

Theorem 4. [9]. *Let $m \equiv 3 (\text{mod } 8)$. Then, $\mathbb{Q}''(\sqrt{m})$ splits into three H-subsets. In particular, $(\sqrt{m}/1)^H$, $(\sqrt{m}/-1)^H$, and $((1 + \sqrt{m})/2)^H$ are at least three H-orbits of $\mathbb{Q}''(\sqrt{m})$.*

Lemma 5. *Every RQIN in $\mathbb{Q}''(\sqrt{m})$ is ambiguous number.*

Theorem 6. [29]. *If $<b_1, b_2, b_2, \cdots, b_k>$ is symmetric continued fraction and if $<b_1, b_2, b_2, \cdots, b_k> = (R + \sqrt{M})/S$, then $M = R^2 + S^2$.*

Theorem 7. [9]. *The set $\mathbb{Q}''(\sqrt{m}) = \{\eta/s : \eta \in \mathbb{Q}^*(\sqrt{m}), s = 1, 2\}$ is unchanged under the action of H.*

Theorem 8. [10]. *Let $m \equiv 1 (\text{mod } 8)$. Then, $\mathbb{Q}''(\sqrt{m})$ splits into four H-subsets. In particular, $(\sqrt{m}/1)^H$, $(\sqrt{m}/-1)^H$, $((1 + \sqrt{m})/2)^H$, and $((1 + \sqrt{m})/4)^H$ are at least four H-orbits of $\mathbb{Q}''(\sqrt{m})$.*

Theorem 9. [9]. *Let $m \equiv 3 (\text{mod } 8)$. Then, $\mathbb{Q}''(\sqrt{m})$ splits into three H-subsets. In particular, $(\sqrt{m}/1)^H$, $(\sqrt{m}/-1)^H$, and $((1 + \sqrt{m})/2)^H$ are at least three H-orbits of $\mathbb{Q}''(\sqrt{m})$.*

Lemma 10. *Every RQIN in $\mathbb{Q}''(\sqrt{m})$ is an ambiguous number.*

Lemma 11. [14]. *$\beta = (a' + \sqrt{m'})/c'$ is an ambiguous number if and only if $c' < 0$ and $b' = (a'^2 - m)/c' > 0$ or $b' = (a'^2 - m)/c' < 0$, and $c' > 0$.*

Remark 12. [9]. Let $\beta(a', b', c') \in Q^*(\sqrt{n'})$ and $m \in \mathbb{N}$. Then,

(1) $(x'y')^m(\beta) = (\beta) + m = (y'^3x')^{-m}(\beta)$.

(2) $(y'x')^m(\beta) = (\beta)/(1 - 2m(\beta)) = (x'y'^3)^{-m}(\beta)$.

(3) $h^m(\beta) = (\beta_1) \in (\beta)^H$.

Remark 13. It should be noted here that for a reduced number $\beta = (a' + \sqrt{m'})/c'$, we have $a' > 0, c' > 0$, and $b' < 0$.

2. Properties of Reduced Quadratic Irrational Numbers in $Q''(\sqrt{m})$

This section is devoted to study the behavior of reduced numbers.

Lemma 14. *If $r \in Q''(\sqrt{m})$ is an RQIN, then $x'(r)$ is an ambiguous number but not RQIN.*

Proof. Let $r = (a' + \sqrt{m})/c'$ be a reduced quadratic irrational number such that $b' < 0, a' > 0$, and $c' > 0$, where $b' = (a'^2 - m)/c'$. Then, by using the Mobius transformation $x'(r) = -1/2r$, we have $x'(r) = (-a' + \sqrt{m})/2b' = (a_1 + \sqrt{m})/b_1$, where $a_1 < 0$ and $b_1 < 0$. Since $b' < 0$ by using Remark 12, $x'(r)$ is not RQIN. □

Theorem 15. . *Let $p \equiv 1$ or $5 (\mathrm{mod}\ 8)$ such that $p - 1 = s^2$. Then, the circuit of a reduced number $r \in ((\lfloor\sqrt{p}\rfloor + \sqrt{p})/2)^H$ has the type $(2\sqrt{p-1})_2, (\sqrt{p-1})_0)$. Moreover, $\bar{r}$, $-r$, and $-\bar{r}$ each exists on the turning points of the circuit and not reduced.*

Proof. $r \in ((\lfloor\sqrt{p}\rfloor + \sqrt{p})/2)^H$, $r = ((\lfloor\sqrt{p}\rfloor + \sqrt{p})/2)$, $(y'^3x')^{\sqrt{p-1}-1}(r) = -\bar{r}$, where $(\sqrt{p-1} - 1)$ is the number of squares inside the circuit. $x'(y'^2x')(-\bar{r}) = -r$ which shows that one circuit is lying between the inside and outside boundary of the circuit. $x'(y'x')^{\sqrt{p-1}-2}(-r) = -\bar{r}$, where $\sqrt{p-1} - 1$ is the number of squares inside the circuit. $y'^2(\bar{r}) = r$ which implies that one of the squares is lying between the inside and outside boundary of the circuit. □

Theorem 16. *For $p \equiv 5$ or $1 (\mathrm{mod}\ 2^3)$ such that $-1 + p = s^2$ and $r = (\lfloor\sqrt{p}\rfloor + \sqrt{p})/2$ be a reduced number, then $\bar{r}$, $-r$, and $-\bar{r}$ map onto the nonreduced number under the action of x'.*

Proof. Let $r = \sqrt{p} + (\lfloor\sqrt{p}\rfloor - 1)/2$ and $-r = (\lfloor\sqrt{p}\rfloor + \sqrt{p})/-2$. By using linear fractional transformation $x' : \beta = -1/\beta$ and Table 1, where $\beta = (a + \sqrt{m})/c$, $x'(-r) = (-(\lfloor\sqrt{p}\rfloor - 1) + \sqrt{p})/c_1 = (a_1 + \sqrt{m})/c_1$ where $a_1 = -(\lfloor\sqrt{p}\rfloor - 1) < 0$. By using Remark 12, it is not a reduced number. Similarly, $x'(-r)$ is not a reduced number. $\bar{r} = (-(\lfloor\sqrt{p}\rfloor - 1) + \sqrt{p})/-2$ and $\beta = x'(-r) = (-(\lfloor\sqrt{p}\rfloor - 1) + \sqrt{p})/c'$; $c' = 2b > 0$ where $b > 0$. By Remark 12, hence β is not a RQIN. □

Theorem 17. *Let $r = (a' + \sqrt{m})/c' \in Q''(\sqrt{m})$ be a RQIN moved to $1/2((a' + \sqrt{m})/c') \in Q''(\sqrt{m})$ under a Mobius transformation x'. Then,*

$$\left(\frac{c' + \sqrt{m}}{a'}\right)^H \cap \left(\frac{a' + \sqrt{m}}{c'}\right)^H = \Phi. \tag{1}$$

Proof. Suppose $(a' + \sqrt{m})/c' \in Q''(\sqrt{n})$ be RQIN under Mobius transformation x' moved to half of their conjugate, i.e., $x'((a' + \sqrt{m})/c') = 1/2(a' - \sqrt{m}/c')$ by using Table 1, as $m = (a')^2 + (c')^2$. By using Theorem 1, $(a' + \sqrt{m})/c'$ and $-1/(2[(a' + \sqrt{m})/c'])$ have symmetric periodic part, since, in the form of continued fraction, every RQIN has unique description. In similar fashion, $(c' + \sqrt{m})/a'$ and $-1/2[(a' - \sqrt{m})/c']$ with symmetric periodic parts are identical. By Lemma 5 $(a' + \sqrt{m})/c'$ and $(c' + \sqrt{m})/a'$ are not identical. Hence, we conclude that

$$\left(\frac{c' + \sqrt{m}}{a'}\right)^H \cap \left(\frac{a' + \sqrt{m}}{c'}\right)^H = \Phi. \tag{2}$$

□

Lemma 18. *Let $\beta = (a' + \sqrt{m})/c' \in Q''(\sqrt{m})$ which moves to half of their conjugate under the linear fractional transformation x'. Then, $Q''(\sqrt{m})$ has at least 2 distinct circuits*

$$\left(\frac{c' + \sqrt{m}}{a'}\right)^H \text{ and } \left(\frac{a' + \sqrt{m}}{c'}\right)^H. \tag{3}$$

Example 1 reflects Lemma 18.

Example 1. Suppose $m = 13$ and $(2 + \sqrt{m})/3 \in Q''(\sqrt{13})$ be reduced quadratic irrational transformed to half of their conjugate under the x$'$ transformation and $(1_1, 2_0, 1_1, 1_2, 1_1, 2_2, 1_1, 1_2)$ is the type of $((2 + \sqrt{m})/3)$. $(3 + \sqrt{m})/2 \in Q''(\sqrt{13})$ be reduced quadratic irrational transformed to half of their conjugate under the x' transformation and $(2_1, 1_o, 3_2, 1_0, 1_1, 1_2, 3_0)$ is the type of $((3 + \sqrt{m})/2)$. It is easy to see that $((2 + \sqrt{m})/3)$ and $((3 + \sqrt{m})/2)$ are not equivalent, so that $((2 + \sqrt{m})/3) \bigcap ((3 + \sqrt{m})/2) = \phi$ as shown in figures below.

Figures 1 and 2 reflect Lemma 18.

Table 1: Under the action of the group H. The images of elements of $Q^*(\sqrt{m})$ [11].

	$\beta = \frac{a' + \sqrt{m}}{c'}$	a'	b'	c'
$x'(\beta)$	$\frac{-1}{2\beta}$	$-a'$	$\frac{-c'}{2}$	$2b'$
$y'(\beta)$	$\frac{-1}{2(\beta+1)}$	$-a' - c'$	$\frac{-c'}{2}$	$2\left(2a' + b' + c'\right)$
$y'^2(\beta)$	$\frac{-(\beta+1)}{(2\beta+1)}$	$-3a' - 2a' - c'$	$2a' + b' + c'$	$4a' + 4b' + c'$
$y'^3(\beta)$	$\frac{-(2\beta+1)}{2\beta}$	$-a' + 2b'$	$\frac{4a' + 4b' + c'}{2}$	$2\left(2a' + b' + c'\right)$
$x'y'(\beta)$	$\beta + 1$	$a' + c'$	$2a' + b' + c'$	c
$x'y'^3(\beta)$	$\frac{\beta}{2\beta+1}$	$a' + 2b'$	b'	$4a' + 4b' + c'$
$y'x'(\beta)$	$\frac{\beta}{1-2\beta}$	$a' - 2b'$	b'	$-4a' + 4b' + c'$
$y'^2x'(\beta)$	$\frac{1-2\beta}{2(-1+\beta)}$	$3a' - 2a' - c'$	$\frac{-4a' + 4b' + c'}{2}$	$2\left(-2a' + b' + c'\right)$
$y'^3x'(\beta)$	$\beta - 1$	$a' - c'$	$-2a' + b' + c'$	c'

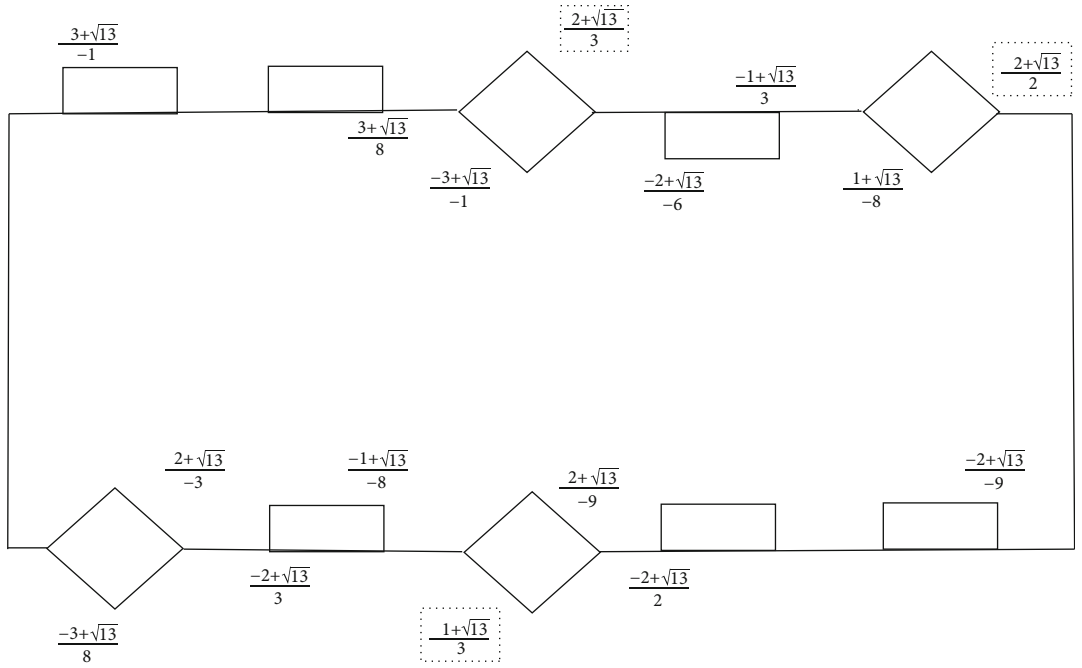

Figure 1: Closed path of $((2+\sqrt{13})/3)^H$.

3. Reduced Length of the H-Circuits of $Q''(\sqrt{P})$

The circuit generates an element of the form $g = (x'y'^{j_k+1})^{m_k} \cdots (x'y'^{j_2+1})^{m_2}(x'y'^{j_1+1})^{m_1}$ of H and fixes some vertex of a square on the closed orbit, and thus, the reduced length of closed orbit is the count of RNs in this closed circuit.

Example 2. The circuit of the type $(1_2, 1_0, 1_2, 1_1, 2_2, 4_0, 2_2, 1_1, 1_2, 1_0, 1_1, 8_0)$ represents that the circuit generates an element $k = (x'y')^8(x'y'^2)(x'y')(x'y'^3)(x'y'^2)(x'y'^3)^2(x'y'^2)(x'y'^3)^2(x'y'^2)(x'y'^3)(x'y')(x'y'^3)$ of H and fixes the vertex $r_1 = 4 + \sqrt{19}$. Suppose $r_1 = 4 + \sqrt{19}$.$\cdots\cdots\cdots(1)$, $(x'y'^3)r_1 = \beta_1$, $(x'y')\beta_1 = (3 + \sqrt{19})/5 = r_2 \cdots\cdots\cdots..(2)$, $(x'y'^3)r_2 = (-1 + \sqrt{19})/9 = \beta_2$, $(x'y'^2)\beta_2 = (2 + \sqrt{19})/10 = \beta_3$, $(x'y'^3)^2\beta_3 = (-4 + \sqrt{19})/2 = \beta_4$, $(x'y')^4\beta_4 = (4 + \sqrt{19})/2 = r_3 \cdots\cdots\cdots..(3)$, $(x'y'^3)^2 r_3 = (-2 + \sqrt{19})/10 = \beta_5$,

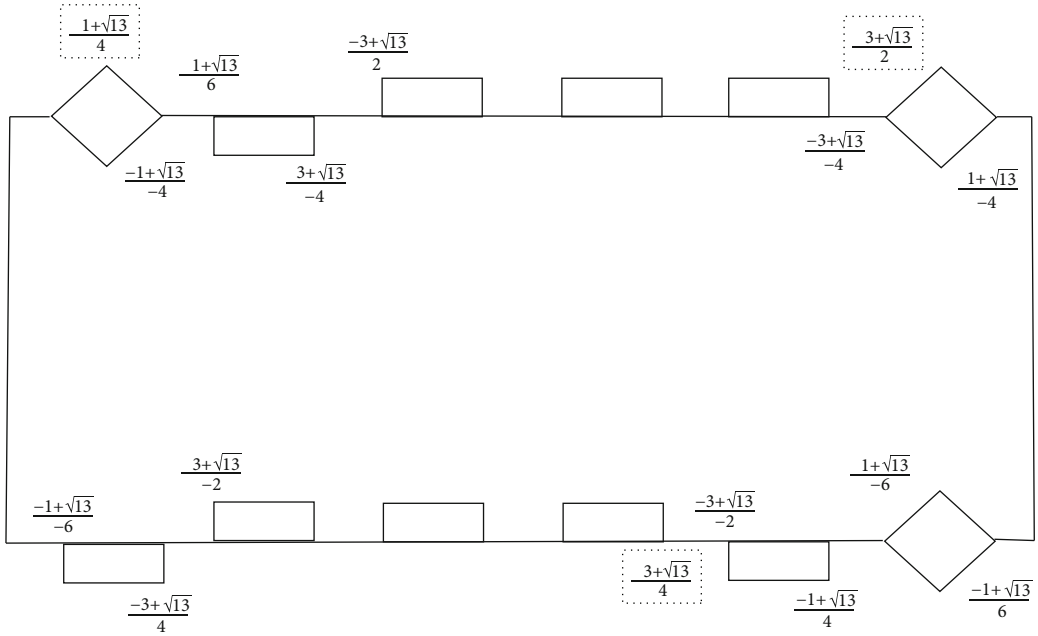

FIGURE 2: Closed path of $((3+\sqrt{13})/2)^H$.

$(x'y'^2)\beta_5 = (1+\sqrt{19})/9 = \beta_6$, $(x'y'^3)\beta_6 = (2+\sqrt{19})/5 = r_4 \cdots ..(4)$, $(x'y'^2)r_4 = -4+\sqrt{19} = \beta_7$, $(x'y'^8)\beta_7 = 4+\sqrt{19} = r_1$. Equations (1), (2), (3), and (4) follow that r_1, r_2, r_3, and r_4 are only reduced numbers in the orbit. Thus, the reduced length of this orbit is 4.

Now, we investigate the reduced cardinalities of H -orbits.

Theorem 19. *Let $p \equiv 1$ or $5 (\mathrm{mod}\ 8)$ such that $p-1 = s^2$ and then the circuit of the reduced number $(((\lfloor\sqrt{p}\rfloor - 1) + \sqrt{p})/2)^H$ has the type $((\sqrt{p-1}-1)_2, 1_1, (\sqrt{p-1}-1)_0, 1_1)$, and $|(((\sqrt{\lfloor\sqrt{p}\rfloor - 1}) + \sqrt{p})/2)^H|_{red} = 1$*

Proof. In order to prove that it is enough to find $k \in H$ in such a manner $k(((\sqrt{\lfloor\sqrt{p}\rfloor - 1}) + \sqrt{p})/2) = (((\sqrt{\lfloor\sqrt{p}\rfloor - 1}) + \sqrt{p})/2)$. The proof was followed by the following four steps: $(y'^3x')^{\sqrt{p-1}-1}(r) = (y'^3x')^{\sqrt{p-1}-1}(((\sqrt{\lfloor\sqrt{p}\rfloor - 1}) + \sqrt{p})/2) = ((-(\sqrt{\lfloor\sqrt{p}\rfloor - 1}) + \sqrt{p})/-2) = -\bar{r}$, $x'(y'^2x')(-\bar{r}) = x'(y'^2x')((-(\sqrt{\lfloor\sqrt{p}\rfloor - 1}) + \sqrt{p})/-2) = (((\sqrt{\lfloor\sqrt{p}\rfloor - 1}) + \sqrt{p})/-2) = -r$, $x'(y'x')^{\sqrt{p-1}-2}y'(-r) = x'(y'x')^{\sqrt{p-1}-2}y'(((\sqrt{\lfloor\sqrt{p}\rfloor - 1}) + \sqrt{p})/-2) = ((-(\sqrt{\lfloor\sqrt{p}\rfloor - 1}) + \sqrt{p})/-2) = \bar{r}$, and $y'^2(\bar{r}) = y'^2((-(\sqrt{\lfloor\sqrt{p}\rfloor - 1}) + \sqrt{p})/-2) = (((\sqrt{\lfloor\sqrt{p}\rfloor - 1}) + \sqrt{p})/2) = r$. Thus, we obtain $y'^2x'(y'x')^{\sqrt{p-1}-2}y'x'(y'^2x')(y'^3x')^{\sqrt{p-1}-1}(((\sqrt{\lfloor\sqrt{p}\rfloor - 1}) + \sqrt{p})/2) = (((\sqrt{\lfloor\sqrt{p}\rfloor - 1}) + \sqrt{p})/2)$. Hence, the circuit of the reduced number $(((\sqrt{\lfloor\sqrt{p}\rfloor - 1}) + \sqrt{p})/2)^H$ has the type $((\sqrt{p-1}-1)_2, 1_1, (\sqrt{p-1}-1)_0, 1_1)$. Now, we have to prove that $|(((\sqrt{\lfloor\sqrt{p}\rfloor - 1}) + \sqrt{p})/2)^H|_{red} = 1$. Let $r = (((\sqrt{\lfloor\sqrt{p}\rfloor - 1}) + \sqrt{p})/2)$ be reduced number. Now, by using Theorem 15 and Theorem 16, the numbers $\bar{r}$,$-\bar{r}$, and $-r$ are on the turning point of the circuit and are not reduced numbers; furthermore, when we will apply linear fractional transformation x' on $\bar{r}$,$-\bar{r}$, and $-r$, then in result, we get no reduced number. So, $(((\sqrt{\lfloor\sqrt{p}\rfloor - 1}) + \sqrt{p})/2)$ is only reduced number in $(((\sqrt{\lfloor\sqrt{p}\rfloor - 1}) + \sqrt{p})/2)^H$. Hence, $|(((\sqrt{\lfloor\sqrt{p}\rfloor - 1}) + \sqrt{p})/2)^H|_{red} 1$. □

Example 3. Take a prime number $p = 17$ such that $17 - 1 = 4^2$ and $17 \equiv 1 (\mathrm{mod}\ 8)$. It is observed from the coset diagram given below that the reduced number $(((\sqrt{\lfloor 17\rfloor} - 1) + \sqrt{17})/2)$ is fixed by the word $(x'y'^2)(y'x')^3(x'y'^2)(y'^3x')^3(((\sqrt{\lfloor 17\rfloor} - 1) + \sqrt{17})/2) = (((\sqrt{\lfloor 17\rfloor} - 1) + \sqrt{17})/2)$; this shows that type of the circuit $(((\sqrt{\lfloor 17\rfloor} - 1) + \sqrt{17})/2)^H$ is $(3_2, 1_1, 3_0, 1_1)$, and it can be seen from the coset diagram given below; $(((\sqrt{\lfloor 17\rfloor} - 1) + \sqrt{17})/2)$ is only reduced number in $(((\sqrt{\lfloor 17\rfloor} - 1) + \sqrt{17})/2)^H$, and hence, $|(((\sqrt{\lfloor 17\rfloor} - 1) + \sqrt{17})/2)^H|_{\mathrm{red}} = 1$

Figure 3 depicted Theorem 19.

Example 4. Take a prime number $p = 101$ such that $p - 1 = 10^2$ and $p \equiv 5 (\mathrm{mod}\ 8)$. It is observed from the coset diagram given below that the reduced number $((\sqrt{\lfloor 101\rfloor} - 1) + \sqrt{101}/2)$ is fixed by the word $(x'y'^2)(y'x')^{10}(x'y'^2)(y'^3x')^{10}((\sqrt{\lfloor 101\rfloor} - 1) + \sqrt{101}/2) = ((\sqrt{\lfloor 101\rfloor} - 1) + \sqrt{101}/2)$; this shows that type of $((\sqrt{\lfloor 101\rfloor} - 1) + \sqrt{101}/2)^H$

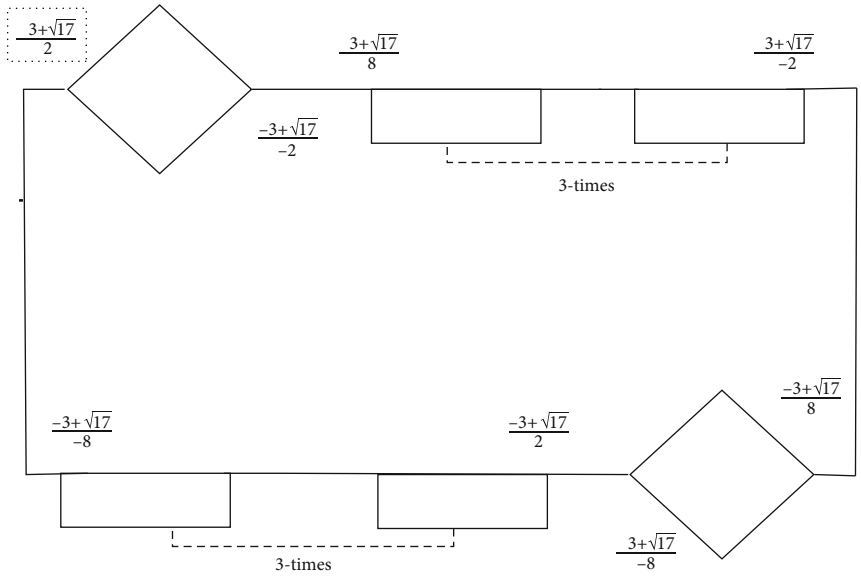

Figure 3: Closed path of $(((\lfloor\sqrt{17}\rfloor - 1) + \sqrt{17})/2)^H$.

of the circuit $((\sqrt{\lfloor 101\rfloor} - 1) + \sqrt{101}/2)^H$ is $(9_2, 1_1, 9_0, 1_1)$, and it can be seen from the coset diagram given below that $((\sqrt{\lfloor 101\rfloor} - 1) + \sqrt{101}/2)$ is only reduced number in $((\sqrt{\lfloor 101\rfloor} - 1) + \sqrt{101}/2)^H$, and hence, $|((\sqrt{\lfloor 101\rfloor} - 1) + \sqrt{101}/2)^H|_{\text{red}} = 1$

Figure 4 reflects Example 4.

Lemma 20. *For $p \equiv 5$ or $3 (\text{mod } 2^3)$ such that $-2 + p = s^2$, then the orbits of reduced numbers $(s + \sqrt{p})^H$ and $((s + \sqrt{p})/4)^H$ have the type $(((s-1)/2)_2, 1_1, (s-1)_0, 1_1, ((s-1)/2)_2, 2s_o)$ and $|(s + \sqrt{p})^H|_{red} = 2 = |((s + \sqrt{p})/4)^H|_{red}$.*

Proof. To show that it is enough to discover $k \in H$ in such a manner $k(r_1) = r_1$, where $r_1 = s + \sqrt{p}.\cdots..(1)$ using Remark 12(1) and (3), we obtain $(x'y')^{-2s}(r_1) = -2s + r_1 = -r + \sqrt{p} = -\bar{(}r_1)$. Now, $(x'y'^3)^{(s-1)/2}(r_1) = ((s-1)(s^2-p) + s + \sqrt{p})/((s-1)[2s^2 + (s^2-p)(s-1)] + 1) = \alpha$ and $(x'y'^3)^{-(s-1)/2}(-\bar{(}r_1)) = (-[(s-1)(s^2-p) + s] + \sqrt{p})/((s-1)[2s + (s^2-p)(s-1)] + 1) = -\bar{(}\alpha)$. In Table 1, $(x'y'^2)(\alpha) = ((s-1)(s^2-p+1) + \sqrt{p})/(-(s^2-p)) = \beta$ and $(x'y'^2)^{-1}(-(\bar{\alpha}))\,((-(s-1)(s^2-p+1) + \sqrt{p})/(-(s^2-p))) = -\bar{\beta} = (r_2) \cdots ..(2)$. Finally, $(x'y')^{-(s-1)}(r_2) = (x'y')^{-(s-1)}(-\bar{\beta}) = ((s-1)(s^2-p+1) + \sqrt{p})/(-(s^2-p)) = \beta$. $(x'y')^{2s}(x'y'^3)^{(s-1)/2}(x'y'^2)(x'y')^{s-1}(x'y'^2)(x'y'^3)^{(s-1)/2}(r_1) = r_1$. Hence, $(((s-1)/2)_2, 1_1, (s-1)_0, 1_1, ((s-1)/2)_2, 2s_o)$ be the type of circuit of reduce number $(s + \sqrt{p})^H$. Similarly, the type of $((s + \sqrt{p})/4)^H$ is same as first one and from equations (1) and (2); hence, $|(s + \sqrt{p})^H|_{\text{red}} = 2 = |((s + \sqrt{p})/4)^H|_{\text{red}}$. □

Example 5. Take a prime number $p = 83$ such that $p - 2 = 9^2$ and $p \equiv 3 (\text{mod } 8)$. It is observed from the coset diagram given below that the reduced number $(9 + \sqrt{83})$ is fixed by the word $(x'y')^{18}(x'y'^3)^4(x'y'^2)(x'y')^8(x'y'^2)(x'y'^3)^4)(9 + \sqrt{83}) = (9 + \sqrt{83})$; this shows that type of the circuit $(9 + \sqrt{83})^H$ is $(4_2, 1_1, 8_0, 1_1, 4_2, 18_0)$, and it can be seen from the coset diagram given below; $(9 + \sqrt{83})$ and $(8 + \sqrt{83})/2$ are only reduced number in $(9 + \sqrt{83})^H$, and hence, $|(9 + \sqrt{83})^H|_{\text{red}} = 2$.

Figure 5 reflects Lemma 20.

Lemma 21. *If $4|p - 3$ and $1 + p = s^2$, then $(\sqrt{p} + \lfloor\sqrt{p}\rfloor)^H$ and $(\sqrt{p}/-1)^H$ circuits have the type (s_o, s_1). Moreover $|(\lfloor\sqrt{p}\rfloor + \sqrt{p})^H|_{red} = 1$ and $|(\sqrt{p}/-1)^H|_{red} = 0$.*

Proof. Similar proof as of Lemma 20. □

Remark 22. (i) It is not necessary that every circuit contains reduced number. As we can see in the figure given below, the circuit of $(\sqrt{p}/-1)$ contains no reduced number.

Figure 6 reflects Remark 22(i).

3.1. Detection of Reduced Numbers. In the orbits of $(s + \sqrt{p})^H$ and $((s + \sqrt{p})/4)^H$ of $Q''(\sqrt{p})$, where $p \equiv 3$ or $5 (\text{mod } 8)$ such that $p - 2 = s^2$, then

(i) $(s + \sqrt{p})$ and $(((s-1) + \sqrt{p})/2)$ are only reduced numbers in the circuit of $(s + \sqrt{p})^H$

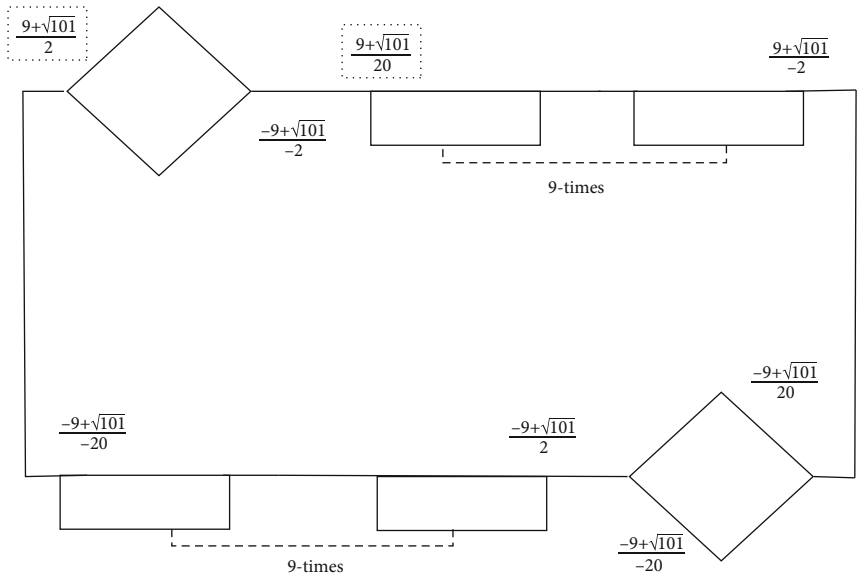

FIGURE 4: Closed path of $((\sqrt{\lfloor 101 \rfloor} - 1) + \sqrt{101}/2)^H$.

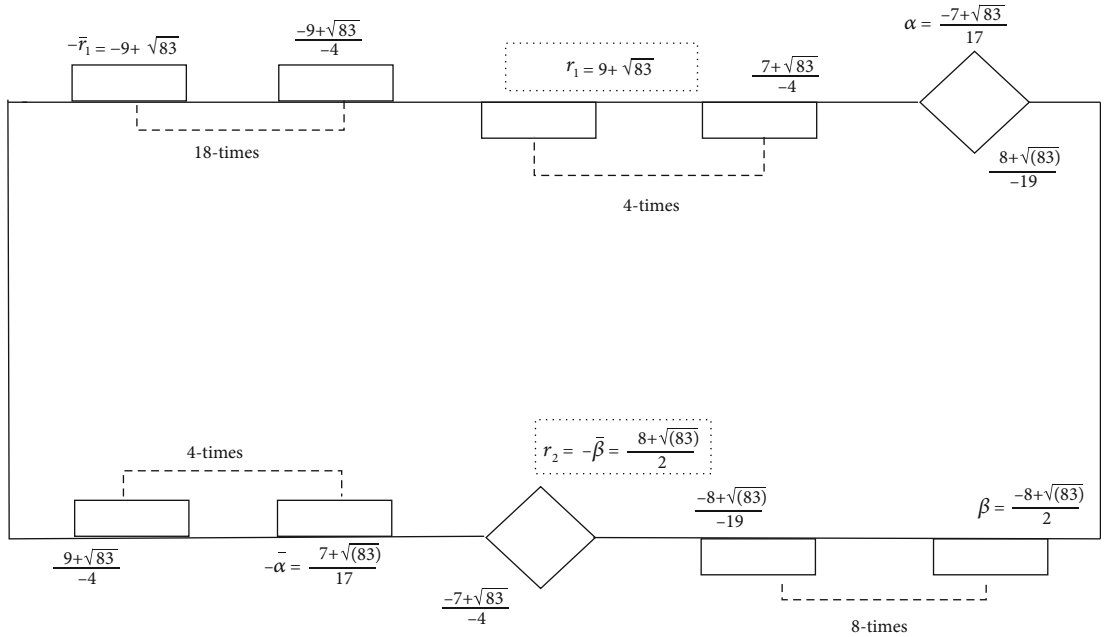

FIGURE 5: Closed path of $(9 + \sqrt{83})^H$.

(ii) $(((s-2) + \sqrt{p})/4)$ and $((s + \sqrt{p})/4)$ are only reduced numbers in the circuit of $((r + \sqrt{p})/4)^H$

$$(s + \sqrt{p})^H \cap \left(\frac{s + \sqrt{p}}{4}\right)^H = \phi. \tag{4}$$

Remark 23. For $p \equiv 3(\text{mod } 2^3)$ such that $-2 + p = s^2$.

(i) If a reduced number $r \in (\sqrt{p} + s)^H$, then its negative conjugate $-\bar{r} \in (\sqrt{p} + s)^H$

(ii) If a reduced number $r \in ((\sqrt{p} + s)/4)^H$ then, its negative conjugate $-\bar{r} \in ((s + \sqrt{p})/4)^H$

Lemma 24. *If $p \equiv 7(\text{mod } 2^3)$ and $2 + p = s^2$ then, the circuit $((s-1) + \sqrt{p})^H$ of the reduced number has the type $(1_1, (((s-1)/2) - 1)_o, 1_2, (s-1)_o, 1_2, (((s-1)/2) - 1)_o, 1_1, 2\ (s-1)_o)$, and hence, $|(s-1) + \sqrt{p})^H|_{red} = 4$*

Proof. To illustrate this, it is sufficient to find $k \in H$ such that $k(r_1) = r_1 \cdots .(i)$, where $r_1 = (s-1) + \sqrt{p}$ by Remark 12,

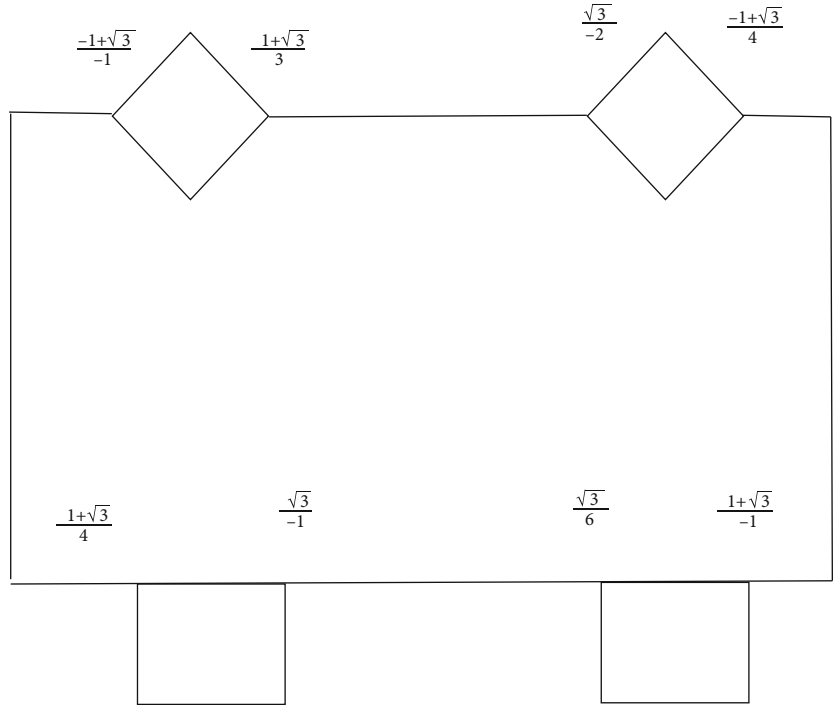

FIGURE 6: Closed path of $(\sqrt{3}/-1)^H$.

then $(x'y')^{-2(s-1)}(r_1) = (x'y')^{-2(s-1)}((s-1)+\sqrt{p}) = -(s-1)+\sqrt{p}) = -\bar{r}_1$; now, by using Table 1. $(x'y'^2)(r_1) = (2(s^2-p)-s+\sqrt{p})/(2(s^2-p)) = \beta_1$ and $(x'y'^2)^{-1}(-\bar{r}_1) = (-2(s^2-p)+s+\sqrt{p})/(2(s^2-p)) = (-\bar{\beta}_1) = r_2 \cdots\cdots\cdots (ii)$, again by (1.1), we have $(x'y')^{(s-3)/2}(r_2) = (x'y')^{(s-3)/2}(-\bar{\beta}_1) = ((s^2-p)(s-1)-s+\sqrt{p})/(2(s^2-p)) = r_3 \cdots\cdots\cdots .(iii)$, and $(x'y')^{-((s-3)/2)}(r_2) = (x'y')^{-((s-3)/2)}(-\bar{\beta}_1) = (-(s^2-p)(s-1)+s+\sqrt{p})/(2(s^2+p)) = -\bar{r}_3$, by Table 1, $(x'y'^3)(r_3) = (s^3+s(b-3)+1+\sqrt{p})/(s^2-p) = \beta_2$ and $(x'y'^{-1})(-\bar{r}_3) = (s^3+s(p+3)-1+\sqrt{p})/(s^2-p) = -\bar{\beta}_2 = r_4 \cdots .(iv)$; finally, $(x'y')^{s-1}(r_4) = ((2s-1)(s^2-p-1)-s+\sqrt{p})/(s^2-p) = \beta_3$, and $\beta_3 = r_4$. Thus, $(x'y')^{2(s-1)}(x'y'^2)(x'y')^{(((s-1)/2)-1)}(x'y'^3)(x'y')^{s-1}(x'y'^3)(x'y')^{(((s-1)/2)-1)}(x'y'^2)(r_1) = r_1$, and from equations (i), (ii), (iii), and (iv), we get $(r_1), r_2, r_3$, and r_4 which are only 4 reduced numbers in the circuit of $((s-1)+\sqrt{p})^H$.

Hence, $|((s-1)+\sqrt{p})^H|_{\text{red}} = 4$. □

Example 6. Take a prime number $p = 79$ such that $p+2 = 9^2$. It is observed from the coset diagram given below that the reduced number $(8+\sqrt{79})$ is fixed by the word $(x'y')^{16}(x'y'^2)(x'y')^3(x'y'^3)(x'y')^8(x'y'^3)(x'y')^3(x'y'^2)(8+\sqrt{79}) = (8+\sqrt{79})$; this shows that type of $(8+\sqrt{79})^H$ of the circuit is $(1_1, 3_0, 1_2, 8_o, 1_2, 3_0, 1_1, 16_o)$, and also, as can be seen from the coset diagram given below, $(8+\sqrt{79})$, $(7+\sqrt{79})/4$, $(8+\sqrt{79})/2$, and $(5+\sqrt{79})/4$ are only reduced number in $(8+\sqrt{79})^H$ and hence $|(8+\sqrt{79})^H|_{\text{red}} = 4$.

Figure 7 reflects Lemma 24.

Lemma 25. *If $p \equiv 7 (\text{mod } 2^3)$ and $2+p = s^2$ then, the circuit $(((s-1)+\sqrt{p})/(2s-3))^H$ of the reduced number has the type $(1_2, ((s-1)/2-1)_o, 1_1, 2(s-1)_o 1_1, ((s-1)/2-1)_o, 1_2, (s-1)_o,)$, and hence, $|(((s-1)+\sqrt{p})/2s-3)^H|_{red} = 2$.*

Proof. Similar proof as of Lemma 24. □

Example 7. Take $p = 167$ such that $p+2 = 13^2$. It is observed from the coset diagram given below that the reduced number $(12+\sqrt{167})/23$ is fixed by the word $(x'y')^{12}(x'y'^3)(x'y')^5(x'y'^2)(x'y')^{24}(x'y'^2)(x'y')^5(x'y'^3)(12+\sqrt{167})/23 = (12+\sqrt{167})/23$; this shows that type of the circuit $((12+\sqrt{167})/23)^H$ is $(12_o, 1_2, 5_0, 1_1, 24_o, 1_1, 5_0, 1_2)$, and it can be seen from the coset diagram given below, $(12+\sqrt{167})/23$ and $(11+\sqrt{167})/23$ and are only reduced numbers in $((12+\sqrt{167})/23)^H$, and hence, $|((12+\sqrt{167})/23)^H|_{\text{red}} = 2$.

Figure 8 reflects Lemma 25.

3.2. Detection of Reduced Numbers. In the circuits of $((s-1)+\sqrt{p})^H$ and $(((s-1)+\sqrt{p})/((2s-3)))^H$ of $Q''(\sqrt{p})$ where $8|p-7$ and $2+p = s^2$, then,

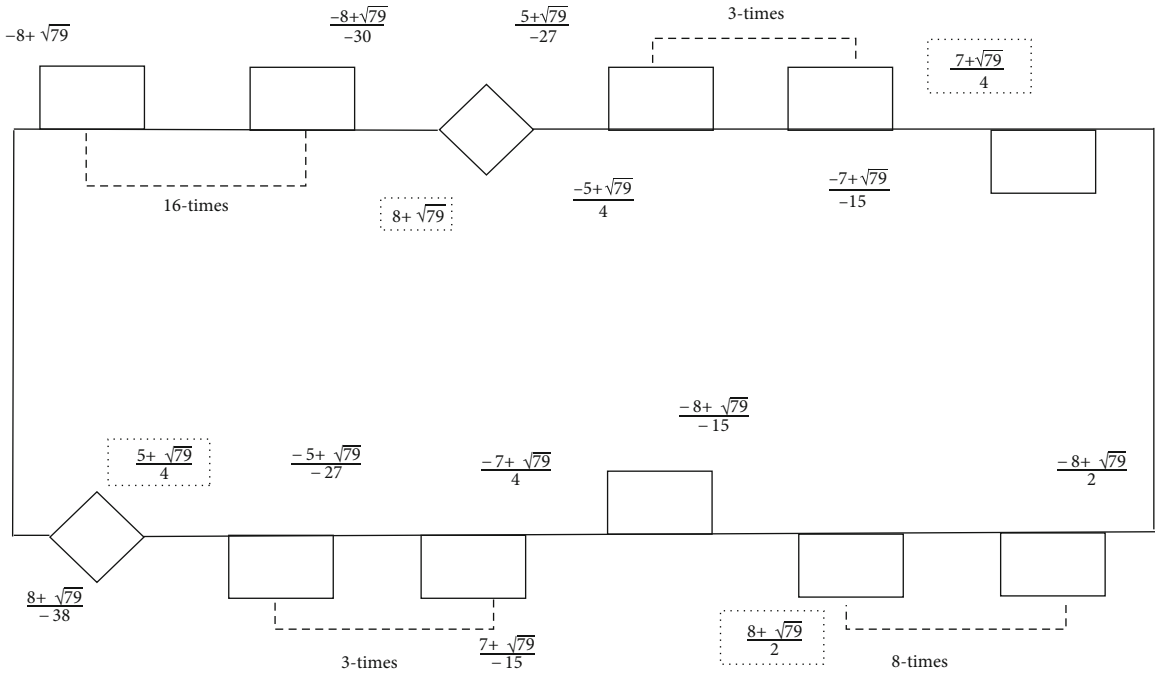

Figure 7: Orbit of $((8+\sqrt{79})/1)^H$ 520703).

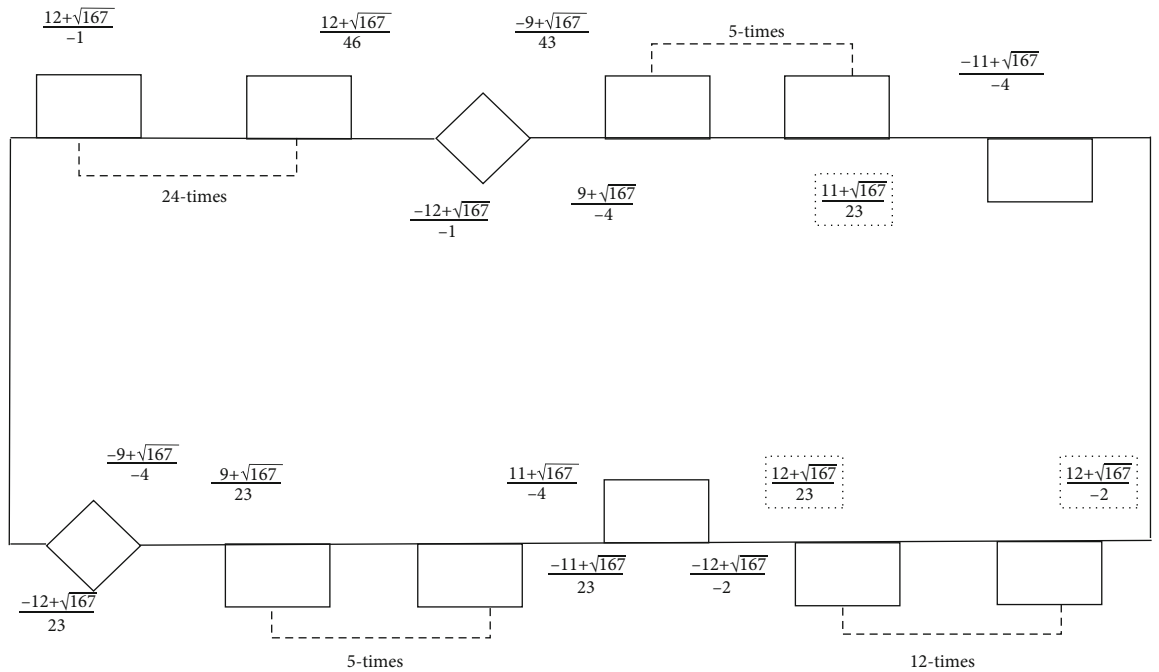

Figure 8: Closed path of $((12+\sqrt{167})/23)^H$.

(i) $((s-1)+\sqrt{p})$, $(((s-2)+\sqrt{p})/4)$, $(((s-1)+\sqrt{p})/2)$, and $(((s-4)+\sqrt{p})/4)$ are only reduced numbers in the circuit of $((s-1)+\sqrt{p})^H$

(ii) $(((s-2)+\sqrt{p})/((2s-3)))$ and $(((s-1)+\sqrt{p})/((2s-3)))$ are only reduced numbers in the circuit of $(((s-2)+\sqrt{p})/((2s-3)))^H$

Remark 26. For $p \equiv 7 (\mathrm{mod}\ 2^3)$ such that $2+p=s^2$.

(1) If $r \in ((s-1)+\sqrt{p})^H$ then $-\bar{r} \in ((s-1)+\sqrt{p})^H$

(2) If $r \in (((s-1)+\sqrt{p})/((2s-3)))^H$, then $-\bar{r} \in (((s-1)+\sqrt{p})/((2s-3)))^H$

(3) $((s-1)+\sqrt{p})^H \bigcap (((s-1)+\sqrt{p})/((2s-3)))^H = \phi.$

4. Conclusion

The idea of types of H-circuits in H-orbits of RQF by Mobius group, which is given in this paper, is new and original. We have presented type of H-circuits with different length in H-orbits $(\beta)^H$, where β is RQIN and H be Mobius group. We have investigated properties of RQINs and classified H-orbits of different length. Furthermore, we proposed reduced length and general form of reduced numbers in different orbits. This work can be extended for the Mobius group $M = <x', y' : x'^2 = y'^6 = 1>$ and $G = <x', y' : x'^2 = y'^3 = 1>$ as well as examined the M-circuits in M-orbits and the G-circuits in G-orbits. Moreover, the reduced length and general form of reduced numbers for different orbits can be discussed.

Data Availability

No real data were used to support this study. The data used in this study are hypothetical, and anyone can use them by citing this article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The authors would like to thank the Deanship of Scientific Research of King Abdulaziz University, Jeddah, Saudi Arabia, for technical and financial support.

References

[1] I. Shahzad, Q. Mushtaq, and A. Razaq, "Construction of new S-box using action of quotient of the modular group for multimedia security," *Security and Communication Networks*, vol. 2019, Article ID 2847801, 13 pages, 2019.

[2] A. Razaq, H. A. Al-Olayan, A. Ullah, A. Riaz, and A. Waheed, "A novel technique for the construction of safe substitution boxes based on cyclic and symmetric groups," *Security and Communication Networks*, vol. 2018, Article ID 4987021, 9 pages, 2018.

[3] A. Razaq, H. Alolaiyan, M. Aehmad et al., "A novel method for generation of strong substitution-boxes based on coset graphs and symmetric groups," *IEEE Access*, vol. 8, pp. 75473–75490, 2020.

[4] A. Razaq, A. Ullah, H. Alolaiyan, and A. Yousaf, "A novel group theoretic and graphical approach for designing cryptographically strong nonlinear components of block ciphers," *Wireless Personal Communications*, vol. 116, no. 4, pp. 1–26, 2020.

[5] M. A. Yousaf, H. Alolaiyan, M. Ahmad, M. Dilbar, and A. Razaq, "Comparison of pre and post-action of a finite abelian group over certain nonlinear schemes," *IEEE Access*, vol. 8, pp. 39781–39792, 2020.

[6] W. Gao, B. Idrees, S. Zafar, and T. Rashid, "Construction of nonlinear component of block cipher by action of modular group PSL(2, Z) on projective line PL(GF(28))," *IEEE Access*, vol. 8, pp. 136736–136749, 2020.

[7] Q. Mushtaq and M. Aslam, "Modular group acting on real quadratic fields," *Bulletin of the Australian Mathematical Society*, vol. 37, no. 2, pp. 303–309, 1988.

[8] Q. Mushtaqr and M. Aslam, "Group generated by two elements of orders 2 and 4 acting on real quadratic fields," *Acta Mathematics Sinica*, vol. 9, no. 1, pp. 48–54, 1993.

[9] M. A. Malik and M. A. Zafar, "Certain H – subsets of $Q(\sqrt{m}) \setminus Q$ under the action of $<x', y' : x'^2 = y'^4 = 1>$," *PUJM*, vol. 64, 2012.

[10] M. A. Zafar and M. A. Malik, "Malik certain type of the orbits of real quadratic fields by Hecke groups," *Mathematical Sciences Letters*, vol. 5, no. 1, pp. 93–97, 2016.

[11] M. A. Malik and M. A. Zafar, "On orbits of $Q(\sqrt{m}) \setminus Q$ under the action of Hecke group $H(\sqrt{2})$," *Middle-East Journal of Scientific Research*, vol. 15, no. 12, pp. 1641–1650, 2013.

[12] A. Razaq, Q. Mushtaq, and A. Yousaf, "The number of circuits of length 4 in PSL $(2, Z)$-space," *Communications in Algebra*, vol. 46, no. 12, pp. 5136–5145, 2018.

[13] A. Razaq, S. Akhter, A. Yousaf, U. Shuaib, and M. Ahmad, "A group theoretic construction of highly nonlinear substitution box and its applications in image encryption," *Multimedia Tools and Applications*, vol. 81, no. 3, pp. 4163–4184, 2022.

[14] S. Ali and M. A. Malik, "Classification of PSL $(2, Z)$-circuits having length six," *Indian Journal of Science and Technology*, vol. 11, no. 42, 2018.

[15] M. A. Malik and S. Ali, "Reduced quadratic irrational numbers and types of G-circuits with length four by modular group," *Indian Journal of Science and Technology*, vol. 11, no. 30, 2018.

[16] T. Chen, M. N. Bari, M. A. Malik, H. M. Afzal Siddiqui, and J. B. Liu, "Icosahedral group and classification of PSL(2, Z)-orbits of real quadratic fields," *Journal of Mathematics*, vol. 2020, Article ID 9568254, 10 pages, 2020.

[17] Q. Mushtaq and S. Anis, "Coset diagram for the action of picard group on $Q(i, \sqrt{3})$," *Algebra Colloquium*, vol. 23, no. 1, pp. 33–44, 2016.

[18] A. Yousaf, H. Alolaiyan, A. Razaq, and M. Younis, "Evolution of ambiguous numbers under the actions of a Bianchi group," *Journal of Taibah University for Science*, vol. 14, no. 1, pp. 615–620, 2020.

[19] A. Razaq, A. Yousaf, U. Shuaib, N. Siddiqui, A. Ullah, and A. Waheed, "A novel construction of substitution box involving coset diagram and a bijective map," *Security and Communication Networks*, vol. 2017, Article ID 5101934, 16 pages, 2017.

[20] A. Azizi, A. Zekhnini, and M. Taous, "On some metabelian 2 -group whose abelianization is of type $(2, 2, 2)$ andapplications," *Journal of Taibah University for Science*, vol. 9, no. 3, pp. 346–350, 2015.

[21] M. Marin, S. Vlase, R. Ellahi, and M. M. Bhatti, "On the partition of energies for the backward in time problem of thermoelastic materials with a dipolar structure," *Symmetry*, vol. 11, no. 7, p. 863, 2019.

[22] M. H. Mateen and M. K. Mahmood, "Power digraphs associated with the congruence $x^n \equiv y(modm)$," *Punjab University Journal of Mathematics*, vol. 51, pp. 93–102, 2019.

[23] M. H. Mateen, M. K. Mahmood, D. Alghazzawi, and J.-B. Liu, "Enumeration of components and cycles of digraph over the

map $x^p \equiv y(modm)$," *AIMS Mathematics*, vol. 6, no. 5, pp. 4581–4596, 2021.

[24] M. H. Mateen, M. K. Mahmood, D. A. Kattan, and S. Ali, "A novel approach to find partitions of Z_m with equal sum subsets via complete graphs," *AIMS Mathematics*, vol. 6, no. 9, pp. 9998–10024, 2021.

[25] M. Haris Mateen and M. Khalid Mahmood, "A new approach for the enumeration of components of digraphs over quadratic maps," *Journal of prime research in mathematics*, vol. 16, no. 2, pp. 56–66, 2020.

[26] M. Haris Mateen, M. Khalid Mahmoud, and S. Ali, "Importance of power digraphs in computer science," in *2019 International Conference on Innovative Computing (ICIC)*IEEE.

[27] M. Haris Mateen, M. Khalid Mahmood, S. Ali, and M. D. A. Alam, "On symmetry of complete graphs over quadratic and cubic residues," *Journal of Chemistry*, vol. 2021, Article ID 4473637, 9 pages, 2021.

[28] H. Alolaiyan, A. Razaq, A. Yousaf, and R. Zahra, "A comprehensive overview on the formation of homomorphic copies in coset graphs for the modular group," *Journal of Mathematics*, vol. 2021, Article ID 3905425, 11 pages, 2021.

[29] S. G. Telang, M. G. Nadkarni, and J. S. Dani, *Number Theory*, Tata McGraw-Hill Publishing Company Limited, 1996.

[30] A. Adler and J. E. Coury, *The Theory of Numbers*, Jones and Bartlett Publishers, Inc., 1995.