REVISITING THE ACTION OF A SUBGROUP OF THE MODULAR GROUP ON IMAGINARY QUADRATIC NUMBER FIELDS

ABDULAZIZ DEAJIM

Abstract. Consider the modular group $PSL(2, \mathbb{Z}) = \langle x, y \mid x^2 = y^3 = 1 \rangle$ generated by the transformations $x : z \mapsto -1/z$ and $y : z \mapsto (z-1)/z$. Let $H$ be the proper subgroup $\langle y, v \mid y^3 = v^3 = 1 \rangle$ of $PSL(2, \mathbb{Z})$, where $v = xyx$. The reference (M. Ashiq and Q. Mushtaq, Actions of a subgroup of the modular group on an imaginary quadratic field, Quasigroups and Related Systems 14 (2006), 133–146) proposed results concerning the action of $H$ on the subset $\{z \in \mathbb{Q} \mid a, b = \frac{a^2 + n}{c}, c \in \mathbb{Z}, c \neq 0\}$ of the imaginary quadratic number field $\mathbb{Q}(\sqrt{-n})$ for a positive square-free integer $n$. In the current article, the author points out and corrects errors appearing in the aforementioned reference. Most importantly, the corrected estimate for the number of orbits arising from this action is given, where symmetries in the orbits play a crucial role in the proof.

1. Introduction

The study of the action of the modular group $PSL(2, \mathbb{Z})$ and its subgroups on various commutative algebraic structures has been common since the works of Graham Higman and his collaborators in the 1980s ([7], [10], [11]). Moreover, various tracks of applications of the action of the modular group (especially in multimedia security) have been appearing recently, see for instance [1], [13], [15], [16], and [17]. This indeed suggests a promising future for the applications of this seemingly purely mathematical topic.

Stothers in [18] showed that the modular group $G = PSL(2, \mathbb{Z})$ has the finite presentation $\langle x, y \mid x^2 = y^3 = 1 \rangle$, where $x$ and $y$ are, respectively, the linear fractional transformations $z \mapsto -1/z$ and $z \mapsto (z-1)/z$. For a square-free integer $m$, the action of $G$ and its subgroups on certain subsets of the quadratic number field $\mathbb{Q}(\sqrt{m})$ has been extensively studied (see for instance [4], [5], [6], [8], [9], [11], [12], [14], and [19]). In particular, Ashiq and Mushtaq (in [8]) studied the proper subgroup $H$ of $G$ generated by the transformations $y$ and $v = xyx : z \mapsto -1/(z+1)$, where they showed that $y^3 = v^3 = 1$ are defining relations for $H$, so $H = \langle y, v \mid y^3 = v^3 = 1 \rangle$.

For a positive square-free integer $n$, consider the following subset of the imaginary quadratic number field $\mathbb{Q}(\sqrt{-n})$:

$$Q^*(\sqrt{-n}) := \left\{ \frac{a + \sqrt{-n}}{c} \mid a, b = \frac{a^2 + n}{c}, c \in \mathbb{Z}, c \neq 0 \right\}.$$  

Deajim and Aslam in [6] studied the action of $G$ on $Q^*(\sqrt{-n})$, in which the main result is counting the orbits resulting from this action. Ashiq and Mushtaq in [2] studied the action of the subgroup $H$ on $Q^*(\sqrt{-n})$, where they suggested a formula to count the orbits resulting from this action. However, the author of this article has found some technical/mathematical mistakes in [2] which invited the need to revisit its findings with the aim of correcting these mistakes and, particularly, giving the correct formula for the number of orbits.

In Section 2, the errors of [2] are listed along with the reasoning for such a judgment. Section 3 aims primarily at correcting the main result of [2], namely [2, Theorem 9], by giving in Theorem 3.5 the accurate formula for the number of orbits arising from the action of $H$ on $Q^*(\sqrt{-n})$. Besides, some lemmas which were used to prove Theorem 3.5 help also in correcting some of the mistakes.
Throughout this article, \( n \) denotes a positive square-free integer.

An element \( \alpha = (a + \sqrt{-n})/c \in \mathbb{Q}^*(\sqrt{-n}) \) is said to be totally positive if \( ac > 0 \), totally negative if \( ac < 0 \), and of norm zero if \( ||\alpha|| = |a| = 0 \). For \( b = (a^2 + n)/c \), it is obvious that \( bc > 0 \) and so \( b \) and \( c \) are always of the same sign.

For every \( \alpha \in \mathbb{Q}^*(\sqrt{-n}) \), denote the \( H \)-orbit \( \{h(\alpha) \mid h \in H\} \) by \( \alpha^H \) and the \( G \)-orbit \( \{g(\alpha) \mid g \in G\} \) by \( \alpha^G \). It is clear that \( \alpha^H \subseteq \alpha^G \). Denote the set of \( H \)-orbits (resp. the set of \( G \)-orbits) in \( \mathbb{Q}^*(\sqrt{-n}) \) by \( \mathcal{O}_{H,n}^H \) (resp. \( \mathcal{O}_{G,n}^G \)).

As usual, we denote by \( \lfloor . \rfloor \) the floor function, by \( d(k) \) the number of positive divisors of \( k \), and by \( d_{\leq i}(k) \), for \( i, k \in \mathbb{N} \) with \( i \leq k \), the number of positive divisors of \( k \) which do not exceed \( i \). For example, \( d(15) = 4 \) and \( d_{\leq 5}(15) = 3 \). Recall that \( d \) is a multiplicative function and, for a prime \( p \), \( d(p^l) = t + 1 \) where \( t \in \mathbb{N} \).

For \( \alpha = (a + \sqrt{-n})/c \in \mathbb{Q}^*(\sqrt{-n}) \), we sometimes use the notation \( a_\alpha \), \( b_\alpha \), and \( c_\alpha \) for \( a \), \( b \), and \( c \) respectively. Throughout the article and without mention, we shall make use of the following table which shows the effect of the action of \( t \in \{x, y, y^2, v, v^2\} \) on \( \alpha \) and can be verified through straightforward computations:

| \( t \) | \( a_t(\alpha) \) | \( b_t(\alpha) \) | \( c_t(\alpha) \) |
|---|---|---|---|
| \( x \) | \(-a\) | \( c\) | \( b\) |
| \( y \) | \(-a + b\) | \(-2a + b + c\) | \( b\) |
| \( y^2 \) | \(-a + c\) | \( c\) | \(-2a + b + c\) |
| \( v \) | \(-a - c\) | \( c\) | \( 2a + b + c\) |
| \( v^2 \) | \(-a - b\) | \( 2a + b + c\) | \( b\) |

Table 1: The action of \( x, y, y^2, v, \) and \( v^2 \)

We summarize below the main errors in [2] with some comments on them.

**Claim 1** [2] line 1 of the proof of Theorem 6:

Let \( \alpha \) be a totally positive imaginary quadratic number. Then, by Theorem 3 (i), \( y(\alpha) \) or \( y^2(\alpha) \) is a totally negative imaginary quadratic number.

Claim 1 is not necessarily true. We show in Lemma 3.1 that if \( \alpha \) is totally positive, then one of \( y(\alpha) \) and \( y^2(\alpha) \) is totally positive and the other is either totally positive, totally negative, or of norm zero. For instance, consider the totally positive element \( \alpha = (2 + \sqrt{-5})/3 \). Then, both \( y(\alpha) = (1 + \sqrt{-5})/3 \) and \( y^2(\alpha) = (1 + \sqrt{-5})/2 \) are totally positive as well. Another example is given by \( \beta = (1 + \sqrt{-1})/2 \), then \( y(\beta) = \sqrt{-1} \) is of norm zero and \( y^2(\beta) = 1 + \sqrt{-1} \) is totally positive. On the other hand, it should also be noted that [2] Theorem 3 (i)] states that \( y(\alpha) \) and \( y^2(\alpha) \) are totally positive when \( \alpha \) is totally negative, which is true, but Claim 1 above strangely misquotes it. Note that Claim 1 being false renders the proof of [2] Theorem 6) false.

**Claim 2** [2] Theorem 8):

(v) If \( \alpha = (1 + \sqrt{-n})/c_1 \) \((n \neq 3)\), where \( 1 + n = c_1c_2 \), \( c_1 \neq 1 \) or \( n + 1 \), then \( \alpha \) is the only element of norm 1 in \( \alpha^H \).
It is strange that their proof of (v) contradicts the statement above, where the authors of [2] stated explicitly that \( y^2(\alpha) = (1 + \sqrt{-n})/(n+1) \) when \( c_1 = 2 \). But then it is obvious that \( y^2(\alpha) \in \alpha^H \) and is of norm 1 with \( \alpha \neq y^2(\alpha)! \) This shows that the statement of (v) is false in general. For instance, consider \( \alpha = (1 + \sqrt{-5})/2 \). Then \( \alpha \) is of norm 1 and satisfies the assumptions of Theorem 8 (v) mentioned above. However, \( y^2(\alpha) = (1 + \sqrt{-5})/3 \) is also of norm 1 belonging to \( \alpha^H \) and is different from \( \alpha \).

As for the other parts of [2, Theorem 8], it is also noted that the arguments in the proof of parts (iii) and (iv) of [2, Theorem 8] are not sufficient although the statements are correct. In fact, parts (iii) and (iv) specify certain cases where an \( H \)-orbit contains only one element of norm zero. Part of the proof of Theorem 8 below. We briefly give here some counter-examples to [2, Theorem 9]. For instance, consider \( \alpha \) odd integers, consider

Claim 3 [2, Theorem 9]:

If \( n \neq 3 \), then the total number of orbits of \( \mathbb{Q}^*(\sqrt{n}) \) under the action of \( H \) are:

(i) \( 2d(n) + 2d(n + 1) - 6 \) if \( n \) is odd, and

(ii) \( 2d(n) + 2d(n + 1) - 4 \) if \( n \) is even.

This is the main result of [2], which is inaccurate. Its proof relies on [2, Theorem 8], which has some gaps (see Claim 2). The correct estimate of the number of orbits is given in Theorem 3.5 below. We briefly give here some counter-examples to [2, Theorem 9]. For odd integers, consider \( n = 1 \) and \( n = 21 \) for instance. For \( n = 1 \), the above estimate gives \( |O^{-1}_H| = -2 \) which is absurd. Our estimate (see Theorem 3.5) gives \( |O^{-1}_H| = 2 \). For \( n = 21 \), the above estimate gives \( |O^{-1}_{21}| = 12 \), whereas our estimate gives \( |O^{-1}_{21}| = 16 \). In fact, according to Theorem 3.5, the number of orbits in this case has to be congruent to zero modulo 8. For even integers, consider \( n = 26 \) for instance. The above estimate gives \( |O^{-1}_{26}| = 16 \), whereas our estimate gives \( |O^{-1}_{26}| = 24 \). The details of the computations of these counter-examples are given just after the proof of Theorem 3.5.

3. Lemmas and Main Result

The main result of the article is to prove Theorem 3.5 which gives the precise estimate for the number of \( H \)-orbits \( |O^{-1}_H| \), correcting [2, Theorem 9]. Besides serving to prove Theorem 3.5, some of the lemmas below contribute also in correcting some of the errors of [2] mentioned in Section 2.

Lemma 3.1. Let \( \alpha = (a + \sqrt{-n})/c \in \mathbb{Q}^*(\sqrt{n}) \).

(1) If \( \alpha \) is totally positive, then one of \( y(\alpha) \) and \( y^2(\alpha) \) is totally positive and the other is either totally positive, totally negative, or of norm zero; whereas both \( v(\alpha) \) and \( v^2(\alpha) \) are totally negative.

(2) If \( \alpha \) is totally negative, then one of \( v(\alpha) \) and \( v^2(\alpha) \) is totally negative and the other is either totally negative, totally positive, or of norm zero; whereas both \( y(\alpha) \) and \( y^2(\alpha) \) are totally positive.

(3) If \( \alpha \) is of norm zero, then both \( y(\alpha) \) and \( y^2(\alpha) \) are totally positive and both \( v(\alpha) \) and \( v^2(\alpha) \) are totally negative.

Proof. Once and for all, note here and elsewhere that Table 1 is used without mention.

(1) Assume that \( a, b, c > 0 \) (the case \( a, b, c < 0 \) is proved similarly). We show first that at least one of \( y(\alpha) \) and \( y^2(\alpha) \) is totally positive. To the contrary, suppose that neither of them is totally positive. If \( y(\alpha) \) is totally negative, then (as \( c_y(\alpha) = b > 0 \)) \( a_y(\alpha) = -a + b < 0 \). As \( b_y^2(\alpha) = c > 0 \) and as \( b_y^2(\alpha) \) and \( c_y^2(\alpha) \) have the same sign, we have \( -a + b - a + c = c_y^2(\alpha) > 0 \) implying that \( a_y^2(\alpha) = -a + c > 0 \) (as \( -a + b < 0 \)). So, \( y^2(\alpha) \) is totally
positive, a contradiction. Similarly, if \( y^2(\alpha) \) is totally negative, then \( y(\alpha) \) is totally positive, a contradiction. On the other hand, if \( y(\alpha) \) is of norm zero, then \( a_y(\alpha) = -a + b = 0 \). So, \( c_y^2(\alpha) = -a + b - a + c = -a + c = a_y^2(\alpha) \) implying that (as \( c_y^2(\alpha) \neq 0 \)) \( a_y^2(\alpha)c_y^2(\alpha) > 0 \) and thus \( y^2(\alpha) \) is totally positive, a contradiction. Similarly, if \( y^2(\alpha) \) is of norm zero, then \( y(\alpha) \) is totally positive, a contradiction. This argument leads to the assertion that at least one of \( y(\alpha) \) and \( y^2(\alpha) \) is totally positive. Suppose that it is \( y(\alpha) \) which is totally positive (if it were \( y^2(\alpha) \), then the proof would be similar). It then follows that \( y^2(\alpha) \) is either totally positive, totally negative, or of norm zero depending respectively on whether \( a_y^2(\alpha) > 0 \), \( a_y^2(\alpha) < 0 \), or \( a_y^2(\alpha) = 0 \). As for \( v(\alpha) \) and \( v^2(\alpha) \), note that having \( a_v(\alpha) = -a - c < 0 \) and \( c_v(\alpha) = 2a + b + c > 0 \) implies that \( v(\alpha) \) is totally negative. Also, having \( a_{v^2}(\alpha) = -a - b < 0 \) and \( c_{v^2}(\alpha) = b > 0 \) implies that \( v^2(\alpha) \) is totally negative.

(2) Similar to the proof of part (1).

(3) Suppose that \( a = 0 \). Then \( a_y(\alpha)c_y(\alpha) = b^2 > 0 \), \( a_y^2(\alpha)c_y^2(\alpha) = bc + c^2 > 0 \) (\( b \) and \( c \) are of the same sign), and so \( y(\alpha) \) and \( y^2(\alpha) \) are totally positive. On the other hand, \( a_v(\alpha)c_v(\alpha) = -bc - c^2 < 0 \), \( a_{v^2}(\alpha)c_{v^2}(\alpha) = -b^2 < 0 \), and so \( v(\alpha) \) and \( v^2(\alpha) \) are totally negative.

We have the following obvious observations (see [6] Lemmas 3.2 and 3.3).

**Lemma 3.2.** ([6] Lemmas 3.2 and 3.3) For \( \alpha = (a + \sqrt{-n})/c \in \mathbb{Q}^*(\sqrt{-n}) \), we have

(i) \( \alpha \) is totally positive if and only if \( x(\alpha) \) is totally negative.

(ii) \( \alpha \) has norm zero if and only if \( x(\alpha) \) has norm zero.

For \( \alpha \in \mathbb{Q}^*(\sqrt{-n}) \), the sets \( \frac{y}{\alpha} = \{\alpha, y(\alpha), y^2(\alpha)\} \) and \( \frac{v}{\alpha} = \{\alpha, v(\alpha), v^2(\alpha)\} \) are called respectively the \( y \)-cycle and the \( v \)-cycle of \( \alpha \) (or just cycles when \( \alpha, y, \) and \( v \) are clear in the context). We call a cycle totally positive (resp. totally negative) if all its elements are totally positive (resp. if all its elements are totally negative).

**Lemma 3.3.** Under the action of \( H \) on \( \mathbb{Q}^*(\sqrt{-n}) \), the following holds for \( \alpha = (a + \sqrt{-n})/c \in \mathbb{Q}^*(\sqrt{-n}) \):

(i) [6] Lemma 3.3] The cycle \( \frac{y}{\alpha} \) is totally positive if and only if either \( a > 0, a < b, a < c \) or \((a < 0, a > b, a > c)\).

(ii) The cycle \( \frac{v}{\alpha} \) is totally negative if and only if either \( a > 0, -a > b, -a > c \) or \((a < 0, -a < b, -a < c)\).

(iii) The cycle \( \frac{y}{\alpha} \) is totally positive if and only if the cycle \( x(\alpha) \) is totally negative.

(iv) If the cycle \( \frac{y}{\alpha} \) is totally positive, then \( \alpha^H \neq x(\alpha)^H \) (i.e. \( \alpha \) and \( x(\alpha) \) belong to distinct \( H \)-orbits).

(v) If \( n \neq 1 \) and \( \alpha \) has norm zero, then \( \alpha^H \neq x(\alpha)^H \).

**Proof.**

(i) This is [6] Lemma 3.3.

(ii) Suppose that \( \frac{v}{\alpha} \) is totally negative. As \( \alpha \) is totally negative, either \( a > 0 \) and \( b, c < 0 \) or \((a < 0 \) and \( b, c > 0)\). Assume that \( a > 0 \) and \( b, c < 0 \). Since \( b_{v(\alpha)} = c < 0 \), we get \( c_{v(\alpha)} < 0 \). As further \( v(\alpha) \) is totally negative, we must then have \( -a - c = a_v(\alpha) > 0 \) and so \( -a > c \). Since also \( c_{v^2}(\alpha) = b < 0 \) and \( v^2(\alpha) \) is totally negative, \( a_{v^2}(\alpha) = -a - b > 0 \) and so \( -a > b \). A similar argument yields that if \( a < 0 \) and \( b, c > 0 \) then \( -a < b \) and \( -a < c \).

Conversely, suppose that \( a > 0 \), \( -a > b \), and \( -a > c \) (the case when \( a < 0 \), \( -a < b \), and \( -a < c \) is handled similarly). Since \( a > 0 \) and \( -a > c \), \( c < 0 \) and so \( \alpha \) is totally negative.
As \( a_{v(\alpha)} = -a - c > 0 \) and \( b_{v(\alpha)} = c < 0 \) and \( b_{v(\alpha)}, c_{v(\alpha)} \) are of the same sign, \( v(\alpha) \) is totally negative too. As \( a_{x(\alpha)} = -a - b > 0 \) and \( c_{x(\alpha)} = b < 0 \), \( v^2(\alpha) \) is totally negative as well. Hence, the cycle \( \frac{v}{\alpha} \) is totally negative.

(iii) Suppose that \( \frac{y}{\alpha} \) is totally positive. By (i), if \( a > 0, b < c, \) and \( c < a, \) then it follows from (ii) that \( x(\alpha) \) is totally negative since \( a_{x(\alpha)} = -a < 0, -a_{x(\alpha)} = a < c = b_{x(\alpha)}, \) and \( -a_{x(\alpha)} = a < b = c_{x(\alpha)}. \) The case when \( a < 0, a > b, \) and \( a > c \) is similar.

Conversely, suppose that \( \frac{v}{\alpha} \) is totally negative. Then by (ii), if \( a_{x(\alpha)} = -a > 0, \)
\( -a_{x(\alpha)} = a > b_{x(\alpha)} = c, \) and \( -a_{x(\alpha)} = a > c_{x(\alpha)} = b, \) then it follows from (i) that \( \frac{y}{\alpha} \) is totally positive. The case when \( a_{x(\alpha)} < 0, -a_{x(\alpha)} < b_{x(\alpha)}, \) and \( -a_{x(\alpha)} < c_{x(\alpha)} \) is similar.

(iv) Suppose that \( \frac{y}{\alpha} \) is totally positive. By (iii), \( \frac{x}{\alpha} \) is totally negative. To show that \( \alpha^H \neq x(\alpha)^H \), we need to show that \( h(\alpha) \neq x(\alpha) \) for any \( h \in H. \) It can be seen that an arbitrary non-identity element of \( H \) takes one and only one of the following forms:

- \( h_1 = y^\epsilon \), for \( \epsilon \in \{1, 2\} \)
- \( h_2 = v^\delta \), for \( \delta \in \{1, 2\} \)
- \( h_3 = y^{e_k}v^{\delta_k} \ldots y^{e_2}v^{\delta_2}y^{e_1}v^{\delta_1}, \) for \( k \geq 1, e_i, \delta_i \in \{1, 2\}, 1 \leq i \leq k \)
- \( h_4 = v^{\delta_k}y^{e_{k-1}+\delta_{k-1}} \ldots y^{e_2}v^{\delta_2}y^{e_1}v^{\delta_1}, \) for \( k \geq 2, e_i, \delta_j \in \{1, 2\}, 1 \leq i \leq k-1, 1 \leq j \leq k \)
- \( h_5 = v^{\delta_k}y^{e_k} \ldots v^{\delta_2}y^{e_2}v^{\delta_1}y^{e_1}, \) for \( k \geq 1, e_i, \delta_i \in \{1, 2\}, 1 \leq i \leq k \)
- \( h_6 = y^{e_k}v^{\delta_{k-1}+\delta_{k-1}} \ldots v^{\delta_2}y^{e_2}v^{\delta_1}y^{e_1}, \) for \( k \geq 2, e_i, \delta_j \in \{1, 2\}, 1 \leq i \leq k, 1 \leq j \leq k-1 \)

The \( h_1 \) case: Since there is no \( z \in \mathbb{C} \) such that \( y^\epsilon(z) = x(z), \) we get \( h_1(\alpha) = y^\epsilon(\alpha) \neq x(\alpha). \) Alternatively, \( y^\epsilon(\alpha) \neq x(\alpha) \) since \( y^\epsilon(\alpha) \) is totally positive and \( x(\alpha) \) is totally negative (by Lemma 3.1).

The \( h_2 \) case: Since there is no \( z \in \mathbb{C} \) such that \( v^\delta(z) = x(z), \) we get \( h_2(\alpha) = v^\delta(\alpha) \neq x(\alpha). \) Alternatively, \( v^\delta(\alpha) \neq x(\alpha) \) since if equality holds then \( xy^\delta(x) = x(\alpha) \) would imply that \( x(\alpha) = y^{-\delta}(\alpha), \) a contradiction (see the \( h_1 \) case above).

The \( h_3 \) case: As \( \alpha \) is totally positive, it follows from Lemma 3.1 (1) that \( v^{e_i}(\alpha) \) is totally negative and so, by Lemma 3.1 (2), \( y^{e_i}v^{\delta_i}(\alpha) \) is totally positive. Repeating this argument for \( i = 1, \ldots, k, \) we get that \( h_3(\alpha) \) is totally positive. Since \( x(\alpha) \) is totally negative, \( h_3(\alpha) \neq x(\alpha). \)

The \( h_4 \) case: If we let \( h_4^* = v^{-\delta_k}h_4 = y^{e_k}v^{\delta_{k-1}} \ldots y^{e_2}v^{\delta_2}y^{e_1}v^{\delta_1}, \) then by an argument similar to that in the \( h_3 \) case, \( h_4^*(\alpha) \) is totally positive. If \( h_4(\alpha) = x(\alpha), \) then \( h_4^*(\alpha) = v^{-\delta_k}x(\alpha) \in \frac{v}{\alpha} \) and so \( h_4^*(\alpha) \) is totally negative, a contradiction.

The \( h_5 \) case: If we let \( h_5^* = v^{-\delta_k}h_5 = y^{e_k}v^{\delta_2}y^{e_2}v^{\delta_1}y^{e_1}, \) then as \( y^{e_1}(\alpha) \) is totally positive, it follows by an argument similar to that in the \( h_3 \) case that \( h_5^*(\alpha) \) is totally positive. If \( h_5(\alpha) = x(\alpha), \) then \( h_5^*(\alpha) = v^{-\delta_k}x(\alpha), \) which is impossible since \( h_5^*(\alpha) \) is totally positive, while \( v^{-\delta_k}x(\alpha) \) is totally negative (see the \( h_4 \) case).

The \( h_6 \) case: If we let \( h_6^* = y^{-e_k}h_6 = v^{\delta_{k-1}+\delta_{k-1}} \ldots v^{\delta_2}y^{e_2}v^{\delta_1}y^{e_1}, \) then as \( y^{e_1}(\alpha) \) is totally positive, it follows by an argument similar to that in the \( h_3 \) case that \( h_6^*(\alpha) \) is totally negative. If \( h_6(\alpha) = x(\alpha), \) then \( h_6^*(\alpha) = y^{-e_k}x(\alpha), \) which is impossible since \( h_6^*(\alpha) \) is totally negative, while \( y^{-e_k}x(\alpha) \) is totally positive by Lemma 3.1 (2).

Now, by having just shown the impossibility of all cases above, we conclude that there is no \( h \in H \) such that \( h(\alpha) = x(\alpha) \) and therefore \( \alpha \) and \( x(\alpha) \) belong to distinct \( H \)-orbits as claimed.
Remark first that we excluded the case \( n = 1 \) since the only elements of \( \mathbb{C} \) fixed by \( x \) are \( \pm \sqrt{-1} \in \mathbb{Q}^*(\sqrt{-1}) \) (i.e. \( x(\pm \sqrt{-1}) = \pm \sqrt{-1} \)); see [6] Lemma 3.4. Let \( n \neq 1 \) and suppose that \( \alpha \) has norm zero. Then, \( x(\alpha) \) has norm zero too. We need to show that \( h(\alpha) \neq x(\alpha) \) for any \( h \in H \). By Lemma 3.1 (3), both \( y(\alpha) \) and \( y^2(\alpha) \) are totally positive, and both \( y(\alpha) \) and \( y^2(\alpha) \) are totally negative. Now, for \( h_1, \ldots, h_6 \) as in (iv), and since none of \( y(\alpha) \), \( y^2(\alpha) \), \( v(\alpha) \), \( v^2(\alpha) \) has norm zero it is easily seen that \( h_i(\alpha) \) is either totally negative or totally positive for every \( i = 1, \ldots, 6 \) (see the argument in (iv)). Thus \( h_i(\alpha) \neq x(\alpha) \) for any \( i = 1, \ldots, 6 \). This settles the claim.

\[ \Box \]

**Example 1.** For \( n = 7 \) and \( \alpha = (-1+\sqrt{-7})/(-4) \), it can be checked that \( y(\alpha) = (-1+\sqrt{-7})/(-2) \), \( y^2(\alpha) = (3+\sqrt{-7})/(-4) \), and so \( \alpha \), \( y(\alpha) \), and \( y^2(\alpha) \) are all totally positive. On the other hand, \( x(\alpha) = (1 + \sqrt{-7})/(-2) \), \( vx(\alpha) = (1 + \sqrt{-7})/(-4) \), and \( v^2x(\alpha) = (3 + \sqrt{-7})/(-4) \) which are all totally negative.

**Lemma 3.4.** ([6] Corollary 3.1) Under the action of \( G \) on \( \mathbb{Q}^*(\sqrt{-n}) \), we have the following:

(i) Every \( G \)-orbit in \( \mathbb{Q}^*(\sqrt{-1}) \) contains a unique element of norm zero.

(ii) Every \( G \)-orbit in \( \mathbb{Q}^*(\sqrt{-2}) \) contains a unique pair of distinct elements of norm zero.

(iii) Every \( G \)-orbit in \( \mathbb{Q}^*(\sqrt{-n}) \), for \( n \geq 3 \), contains either a unique pair of distinct elements of norm zero or a unique totally positive cycle, but not both.

The aim of our main result below is to compute the cardinality \( |O^H_n| \) correcting the estimate given in [2, Theorem 9] (see Claim 3 in Section 2). In particular, we utilize the above results to simply show that

\[ |O^H_1| = |O^G_1|, \text{ and } |O^H_n| = 2|O^G_n| \text{ for } n \geq 2, \]

and then make use of the precise estimate of \( |O^G_n| \) given in [6] Theorem 2.1 for all \( n \geq 1 \).

**Theorem 3.5.** Under the action of \( H \), the number of orbits in \( \mathbb{Q}^*(\sqrt{-n}) \) is

\[
|O^H_n| = \begin{cases} |O^G_1|, & \text{if } n = 1 \\ 2|O^G_n|, & \text{if } n \geq 2 \\ 2d(n) + \frac{1}{2} \sum_{i=1}^{(n-1)/2} |d(i^2 + n) - 2d_{\leq i}(i^2 + n)|, & \text{if } n > 3. \end{cases}
\]

Moreover, \( |O^H_n| \equiv 0 \pmod{8} \) for \( n \geq 3 \).

**Proof.** We begin with the case \( n \geq 2 \), where we show that \( |O^H_n| = 2|O^G_n| \). We show this equality by showing that every \( G \)-orbit splits into two distinct \( H \)-orbits. Let \( \alpha^G \in \mathbb{Q}^G_n \). We know from Lemma 3.4 (ii, iii) that \( \alpha^G \) either contains a unique pair of distinct elements of norm zero or a unique totally positive cycle, but not both. We proceed by dealing with these two possibilities.

Firstly, suppose that \( \alpha^G \) contains a unique pair of distinct elements \( \beta \) and \( x(\beta) \) of norm zero. Since \( \beta \neq x(\beta) \) in this case, we get from Lemma 3.3 (v) that it cannot be the case that both elements belong to \( \alpha^H \). We show that \( \alpha^G \) splits into two distinct \( H \)-orbits \( \alpha^H \) and \( \beta^H \) or \( \alpha^H \) and \( x(\beta)^H \) by showing that \( \alpha^H \) must contain one and only one of these two norm-zero elements while the other belongs to \( \alpha^G - \alpha^H \). If \( \beta \in \alpha^H \), then (by Lemma 3.3 (v)) \( \alpha^G \) is the disjoint union of \( \alpha^H \) and \( x(\beta)^H \) and we are done. Similarly, if \( x(\beta) \in \alpha^H \), then \( \alpha^G \) is the disjoint union of \( \alpha^H \) and \( \beta^H \). Now, it remains to show that one of \( \beta \) or \( x(\beta) \) must belong to \( \alpha^H \). Assume that \( \beta \notin \alpha^H \); we show that \( x(\beta) \in \alpha^H \). Since \( \alpha \in \alpha^G - \alpha^H \), there is some \( g \in G - H \) such that \( \beta = g(\alpha) \). In order
to show that $x(\beta) \in \alpha^H$, we argue that $xg \in H$, which then would imply that $x(\beta) = xg(\alpha) \in \alpha^H$ as desired. Keeping in mind the forms $h_0 = 1$ and $h_1, \ldots, h_6$ that elements of $H$ can take (see the proof of Lemma 3.3 (iv)), we see that $g$, as an element of $G$ but not an element of $H$, can take one of the forms $xh_i$, $h_ix$, $y^\gamma xh_i$, or $h_ixy^\gamma$ for an appropriate $h_i$, $i = 0, \ldots, 6$, $\gamma \in \{1, 2\}$. We do the following argument that exhausts all possible cases.

If $g = xh_i$, then $xg = h_i \in H$ for $i = 0, \ldots, 6$.
If $g = y^\gamma xh_i$, then $xg = xy^\gamma xh_i = y^\gamma h_i \in H$ for $i = 0, \ldots, 6$.
If $g = h_ix$, then $xg = x \in H$.
If $g = h_0xy^\gamma$, then $xg = y^\gamma \in H$.
If $g = h_1x$, then $xg = xy^\gamma \in H$.
If $g = h_1xy^\gamma$, then $xg = xy^\gamma = v^\varepsilon y \in H$.
If $g = h_2x = v^\varepsilon x = v^\varepsilon \in H$.

We have, so far, proved that $\gamma \in \alpha^H$. Similarly, if $x(\beta) \notin \alpha^H$, then $\beta \in \alpha^H$.

Secondly, suppose that $\alpha^G$ contains a unique totally positive cycle $\beta$. By Lemma 3.3 (iii), $\alpha^G$ is a totally negative cycle which is obviously contained in $\alpha^G$. Note also, by Lemma 3.3 (iv), that it cannot be the case that both cycles are contained in $\alpha^H$. Following exactly the same argument of the zero-norm elements above, we conclude that $\alpha^G$ is either the disjoint union of $\alpha^H$ and $\beta^H$ or is the disjoint union of $\alpha^H$ and $x(\beta)^H$, and therefore $\alpha^G$ splits into two distinct $H$-orbits in this case as well.

We have, so far, proved that $|O^H_n| = 2|O^G_n|$ for $n \geq 2$. The proof would by complete in this case by applying [5, Theorem 2.1], which precisely gives the value of $|O^G_n|$ as follows:

$$|O^G_n| = \begin{cases} 
2 & \text{if } n = 2 \\
4 & \text{if } n = 3 \\
d(n) + \frac{2}{3} \sum_{i=1}^{(n-1)/2} [d(i^2 + n) - 2d(i^2 + n)], \text{otherwise.}
\end{cases}$$

and, moreover, declares the congruence $|O^G_n| \equiv 0 \pmod{4}$ for $n \geq 3$.

Finally, for the case $n = 1$, the only elements of norm zero in $\mathbb{Q}^*(\sqrt{-1})$ are $\pm \sqrt{-1}$, and both are fixed by $x$ (see the proof of Lemma 3.3 (v)). We also have by Lemma 3.3 (i) that $\alpha^G$ contains a unique element of norm zero; that is $\alpha^H$ must contain either $-1$ or $-1$ but not both. Suppose that $\sqrt{-1} \in \alpha^G$. If $\sqrt{-1} \notin \alpha^H$, then, by following the argument in the second paragraph of this proof, $x(\sqrt{-1}) \in \alpha^H$. But $x(\sqrt{-1}) = -1$, a contradiction. Thus, $\sqrt{-1} \in \alpha^H$. Similarly, if $-\sqrt{-1} \in \alpha^G$, then $-\sqrt{-1} \in \alpha^H$. This shows that $\alpha^H = \alpha^G$ and hence $|O^H_1| = |O^G_1|$, which in turn equals 2 (by [5, Theorem 2.1]).

**Remark.** We present below some examples showing that the formulas given by [2, Theorem 9] are incorrect in general (see Claim 3 in Section 2).

1. For $n = 1$, the number of orbits $|O^2_1|$ given by [2, Theorem 9] is

$$2d(1) + 2d(2) - 6 = 2[1 + 4 - 6] = -2,$$

which is absurd. By Theorem 3.5, however, $|O^2_1| = 2$. 

2. For \( n = 21 \), the number of orbits \( |O_{21}^H| \) given by [2, Theorem 9] is
\[
2[d(21) + 2d(22) - 6] = 2[4 + 8 - 6] = 12.
\]
This estimate immediately appears to be wrong when tested using the congruence relation in Theorem 3.5. Nonetheless, Theorem 3.5 gives precisely the following estimate
\[
|O_{21}^H| = 2d(21) + \frac{4}{3} \sum_{i=1}^{10} [d(i^2 + 21) - 2d_{\leq i}(i^2 + 21)]
\]
\[
= 8 + \frac{4}{3} \{d(22) - 2d_{\leq 1}(22) + d(25) - 2d_{\leq 2}(25) + d(30) - 2d_{\leq 3}(30) + d(37) - 2d_{\leq 4}(37)
\]
\[+ d(46) - 2d_{\leq 5}(46) + d(57) - 2d_{\leq 6}(57) + d(70) - 2d_{\leq 7}(70) + d(85) - 2d_{\leq 8}(85)
\]
\[+ d(102) - 2d_{\leq 9}(102) + d(121) - 2d_{\leq 10}(121)\}
\]
\[
= 8 + \frac{4}{3} \{4 - 2 + 3 - 2 + 8 - 6 + 2 - 2 + 4 - 4 + 4 - 4 + 8 - 8 + 4 - 4 + 8 - 8 + 3 - 2\}
\]
\[
= 8 + 8 = 16.
\]
3. For \( n = 26 \), the number of orbits \( |O_{26}^H| \) given by [2, Theorem 9] is
\[
2[d(26) + 2d(27) - 4] = 2[4 + 8 - 4] = 16.
\]
Theorem 3.5 gives precisely the following estimate
\[
|O_{26}^H| = 2d(26) + \frac{4}{3} \sum_{i=1}^{12} [d(i^2 + 26) - 2d_{\leq i}(i^2 + 26)]
\]
\[
= 8 + \frac{4}{3} \{d(27) - 2d_{\leq 1}(27) + d(30) - 2d_{\leq 2}(30) + d(35) - 2d_{\leq 3}(35)
\]
\[+ d(42) - 2d_{\leq 4}(42) + d(51) - 2d_{\leq 5}(51) + d(62) - 2d_{\leq 6}(62)
\]
\[+ d(75) - 2d_{\leq 7}(75) + d(90) - 2d_{\leq 8}(90) + d(107) - 2d_{\leq 9}(107)
\]
\[+ d(126) - 2d_{\leq 10}(126) + d(147) - 2d_{\leq 11}(147) + d(170) - 2d_{\leq 12}(170)\}
\]
\[
= 8 + \frac{4}{3} \{4 - 2 + 8 - 4 + 4 - 2 + 8 - 6 + 4 - 4 + 4 - 4 + 6 - 6 + 12 - 10 + 2 - 2
\]
\[+ 12 - 12 + 6 - 6 + 8 - 8\}
\]
\[
= 8 + 16 = 24.
\]

4. Conclusion

Consider the subgroup \( H = \langle y, v \mid y^3 = v^3 = 1 \rangle \) of \( \text{PSL}(2, \mathbb{Z}) = \langle x, y \mid x^2 = y^3 = 1 \rangle \), where \( x : z \mapsto -1/z, y : z \mapsto (z-1)/z \), and \( v = xyx : z \mapsto -1/(z+1) \). For a square-free \( n \in \mathbb{N} \), it is shown that the number of orbits in the set
\[
\mathbb{Q}^*(\sqrt{-n}) = \{ \frac{a + \sqrt{-n}}{c} \in \mathbb{Q}^*(\sqrt{-n}) \mid a, b = \frac{a^2 + n}{c}, c \in \mathbb{Z}, c \neq 0 \},
\]
under the action of \( H \), is given as follows:

\[
\begin{cases}
\frac{2}{3}, & \text{if } n = 1 \\
\frac{4}{3}, & \text{if } n = 2 \\
\frac{8}{3}, & \text{if } n = 3 \\
2d(n) + \frac{4}{3} \sum_{i=1}^{[(n-1)/2]} [d(i^2 + n) - 2d_{\leq i}(i^2 + n)] & , \text{if } n > 3
\end{cases}
\]
and is congruent to 0 modulo 8 for all $n \geq 3$, where $d(k)$ denotes the number of positive divisors of $k$, $d_{\leq i}(k)$ denotes the number of positive divisors of $k$ which do not exceed $i$ for $i, k \in \mathbb{N}$ with $i \leq k$, and $\lfloor \cdot \rfloor$ is the floor function.

References

[1] H. Alolaiyan, A. Razaq, A. Yousaf, and R. Zahra, A comprehensive overview of the formation of homomorphic copies in coset graphs for the modular group, Journal of Mathematics, vol. 2021, Article ID 3905425, 11 pages, 2021. https://doi.org/10.1155/2021/3905425.

[2] M. Ashiq and Q. Mushtaq, Actions of a subgroup of the modular group on an imaginary quadratic field, Quasigroups and Related Systems 14 (2006), 133–146.

[3] M. Ashiq and Q. Mushtaq, Finite presentation of a linear-fractional group, Alg. Colloq. 12 (2005), 585–589.

[4] T. Chen, M. Bari, M. Malik, H. Siddiqui, J-B. Liu, Icosahedral group and classification of $PSL(2, \mathbb{Z})$-orbits of real quadratic fields, Journal of Mathematics, vol. 2020, Article ID 9568254, 10 pages, 2020. https://doi.org/10.1155/2020/9568254.

[5] A. Deajim, The Hecke group $H(\lambda_4)$ acting on imaginary quadratic number fields, Journal of Mathematics, vol. 2021, Article ID 9323424, 11 pages, 2021. https://doi.org/10.1155/2021/9323424.

[6] A. Deajim and M. Aslam, On the number of orbits arising from the action of $PSL(2, \mathbb{Z})$ on imaginary quadratic number fields, U.P.B. Sci. Bull., Series A 82 (2020), 61–74.

[7] G. Higman and Q. Mushtaq, Coset diagrams and relations for $PSL(2, \mathbb{Z})$, Arab Gulf J. Sci. Res., 1 (1983), 159–164.

[8] M. Malik and M. Riaz, Orbits of $\mathbb{Q}^*(\sqrt{m})$ under the action of the modular group $PSL(2, \mathbb{Z})$, U.P.B. Sci. Bull. Series A, 74 (2012), 109-116.

[9] M. Malik and A. Zafar, Real quadratic irrational numbers and modular group action, South East Asian Bull. Math, 35 (2011), 439-445.

[10] Q. Mushtaq, Coset Diagrams for the Modular Group, Ph.D. Thesis, University of Oxford, UK, 1983.

[11] Q. Mushtaq, Modular group acting on real quadratic fields, Bull. Austral. Math. Soc. 37 (1988), 303–309.

[12] Q. Mushtaq, On word structure of the modular group over finite and real quadratic fields, Disc. Math., 178 (1998), 155-164.

[13] A. Razaq, A. Yousaf, U. Shuaib, A. Siddiqui, Atta Ullah, 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. https://doi.org/10.1155/2017/5101934.

[14] A. Razaq, Action of the group $\langle x, y : x^2 = y^6 = 1 \rangle$ on imaginary quadratic fields, Quasigroups and Related Systems, 26 (2018), 139-148.

[15] A. Razaq, H. Alolaiyan, M. Ahmad, M. Yousaf, U. Shuaib, W. Aslam, and M. Alawida, A novel method for generation of strong substitution-boxes based on coset graphs and symmetric groups, IEEE Access, 8 (2020), 75473–75490.

[16] A. Razaq, S. Akhtar, A. Yousaf, U. Shuaib, and M. Ahmad, A group theoretic construction of highly nonlinear substitution box and its applications in image encryption, Multimed Tools Appl, 81 (2022), 4163–4184.

[17] I. Shahzad, Q. Mushtaq, and A. Razaq, Construction of new S-boxes using action of the modular group for multimedia security, Security and Communication Networks, vol. 2019, Article ID 2847801, 13 pages, 2019. https://doi.org/10.1155/2019/2847801.

[18] W. Stothers, Subgroups of the modular group, Proc. Camb. Philos. Soc. 75 (1974), 139–154.

[19] A. Yousaf, H. Alolaiyan, A. Razaq, and M. Younis, Evolution of ambiguous numbers under the actions of a Binachi group, J. Taibah Univ. Sci., 14 (2020), 615–620.

Department of Mathematics, King Khalid University, P.O. Box 9004, Abha, Saudi Arabia

Email address: deajim@gmail.com