ON THE NUMBER OF ORBITS ARISING FROM THE ACTION OF PSL$(2,\mathbb{Z})$ ON IMAGINARY QUADRATIC NUMBER FIELDS

Abdulaziz Deajim[1], Muhammad Aslam[2]

For square-free positive integers n, we study the action of the modular group $PSL(2,\mathbb{Z})$ on the subsets $\{\frac{a+\sqrt{-n}}{c} \in \mathbb{Q}(\sqrt{-n}) \,|\, a, \frac{a^2+n}{c}, c \in \mathbb{Z}\}$ of the imaginary quadratic number fields $\mathbb{Q}(\sqrt{-n})$. In particular, we compute the number of orbits of this action and show, for $n > 3$, that it is equal to

$$d(n) + \frac{2}{3} \sum_{i=1}^{\lfloor \frac{n-1}{2} \rfloor} [d(i^2+n) - 2d_{\leq i}(i^2+n)],$$

where $d(k)$ is the number of positive divisors of k, and $d_{\leq i}(k)$ is the number of positive divisors of k which do not exceed i. We also provide a C++ code to calculate these numbers for square-free integers n with $1 \leq n \leq 100$.

Keywords: imaginary quadratic field, modular group, orbit.
MSC2020: 05A18, 05E18, 11R11, 11A25, 20F05.

1. Introduction

Throughout this paper, we denote by G the modular group $\mathrm{PSL}(2,\mathbb{Z})$, whose elements are all the Möbius transformations $z \mapsto (az+b)/(cz+d)$, $a,b,c,d \in \mathbb{Z}$, $ad-bc=1$. It is known that G has the finite presentation $\langle x, y : x^2 = y^3 = 1\rangle$, where x and y are, respectively, the transformations $z \mapsto -1/z$ and $z \mapsto (z-1)/z$ (see [3] for a proof that uses coset diagrams). The modular group belongs to a more general family of groups called Hecke groups. The Hecke group H_n, $3 \leq n \in \mathbb{N}$, is the group generated by the two Möbius transformations $z \mapsto -1/z$ and $z \mapsto z + \lambda_n$, where $\lambda_n = 2\cos(\pi/n)$. It can be shown that $G \cong H_3$. Actions of the modular group, and Hecke groups in general, on many discrete and non-discrete structures play significant roles in different branches of mathematics (see [4]).

Among the important discrete structures upon which the modular group acts are quadratic number fields. Let $\mathbb{Q}(\sqrt{n})$ be a real quadratic number field, where n is a square-free positive integer. Q. Mushtaq (in [7]) studied the action of G on the following subset of $\mathbb{Q}(\sqrt{n})$:

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

Subsequent works by several authors considered properties emerging from this action (see for instance [5], [6], and [8]).

[1] Associate Professor, Department of Mathematics, King Khalid University, P.O. Box 9004, Abha, Saudi Arabia, e-mail: `deajim@kku.edu.sa, deajim@gmail.com`

[2] Associate Professor, Department of Mathematics, King Khalid University, P.O. Box 9004, Abha, Saudi Arabia, e-mail: `draslamqau@yahoo.com`

We shift the emphasis in this work towards studying the action of the modular group on *imaginary* quadratic number fields. Throughout this paper, n denotes a square-free positive integer. It is not hard to see that there is a natural action of G on $\mathbb{Q}(\sqrt{-n})$ (inherited from the action of G on $\mathbb{C}$ by Möbius transformations). Consider the following subset of the imaginary quadratic number field $\mathbb{Q}(\sqrt{-n})$:

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

It can be checked that $\mathbb{Q}^*(\sqrt{-n})$ is the collection of the complex roots of all quadratic polynomials of the form $cx^2 - 2ax + b$ of the fixed discriminant $-4n$, with $a, b, c \in \mathbb{Z}$ and $0 \leq a^2 < bc$. The aim of this paper is to study the action of G on $\mathbb{Q}^*(\sqrt{-n})$ and, in particular, count the number of orbits in $\mathbb{Q}^*(\sqrt{-n})$ emerging from this action and present an interesting congruence property of this number (Theorem 2.1).

In studying the action of similar groups on imaginary quadratic number fields, the following should be recorded. M. Ashiq and Q. Mushtaq (in [1]) studied the action of the subgroup $\langle u, v : u^3 = v^3 = 1\rangle$ of G on $\mathbb{Q}^*(\sqrt{-n})$ (here $u = y$ and $v = xyx$), where they computed the number of orbits in the subset $\mathbb{Q}^*(\sqrt{-n})$ under this action. A. Razaq (in [9]) studied the action of the group $\langle x, y : x^2 = y^6 = 1\rangle$ on $\mathbb{Q}(\sqrt{-n})$, where he computed the number of orbits in the subset $\left\{ \frac{a+\sqrt{-n}}{3c} \in \mathbb{Q}(\sqrt{-n}) \mid a, \frac{a^2+n}{3c}, c \in \mathbb{Z} \right\}$.

2. The action of G on $\mathbb{Q}^*(\sqrt{-n})$

For $\alpha = \frac{a+\sqrt{-n}}{c} \in \mathbb{Q}^*(\sqrt{-n})$, we use the notation $a_\alpha := a$, $b_\alpha := b = \frac{a^2+n}{c}$, and $c_\alpha := c$.

Proposition 2.1. *$\mathbb{Q}^*(\sqrt{-n})$ is a G-set.*

Proof. As G acts on $\mathbb{Q}(\sqrt{-n})$, it remains only to show that $\mathbb{Q}^*(\sqrt{-n})$ is invariant under this action. Let $\alpha = \frac{a+\sqrt{-n}}{c} \in \mathbb{Q}^*(\sqrt{-n})$. To show that $g(\alpha) \in \mathbb{Q}^*(\sqrt{-n})$ for every $g \in G$, it suffices to show that $x(\alpha), y(\alpha) \in \mathbb{Q}^*(\sqrt{-n})$ since $\{x, y\}$ is a complete set of generators of G. We see, first, that

$$x(\alpha) = \frac{-1}{\alpha} = \frac{-c}{a+\sqrt{-n}} = \frac{-c(a-\sqrt{-n})}{a^2+n} = \frac{-a+\sqrt{-n}}{b}.$$

Now, $a_{x(\alpha)} = -a \in \mathbb{Z}$, $c_{x(\alpha)} = b \in \mathbb{Z}$, and $b_{x(\alpha)} = \frac{a^2_{x(\alpha)}+n}{c_{x(\alpha)}} = \frac{a^2+n}{b} = c \in \mathbb{Z}$, we get that $x(\alpha) \in \mathbb{Q}^*(\sqrt{-n})$. Similarly, we see that

$$y(\alpha) = 1 - \frac{1}{\alpha} = 1 + x(\alpha) = \frac{(-a+b)+\sqrt{-n}}{b}.$$

As $a_{y(\alpha)} = -a + b \in \mathbb{Z}$, $c_{y(\alpha)} = b \in \mathbb{Z}$, and

$$b_{y(\alpha)} = \frac{a^2_{y(\alpha)}+n}{c_{y(\alpha)}} = \frac{(-a+b)^2+n}{b} = -2a + b + \frac{a^2+n}{b} = -2a + b + c \in \mathbb{Z},$$

we get that $y(\alpha) \in \mathbb{Q}^*(\sqrt{-n})$ as well. □

Remark 2.1. For some use in the sequel, the following table summarizes the action of each $g \in \{x, y, y^2\}$ on an arbitrary element $\alpha = \frac{a+\sqrt{-n}}{c} \in \mathbb{Q}^*(\sqrt{-n})$. The first two lines of the table were verified in the above proof, while the third line can be checked in a similar manner.

$g(\alpha)$	$a_{g(\alpha)}$	$b_{g(\alpha)}$	$c_{g(\alpha)}$
$x(\alpha)$	$-a$	c	b
$y(\alpha)$	$b-a$	$-2a+b+c$	b
$y^2(\alpha)$	$c-a$	c	$-2a+b+c$

Table 1: Signatures of $x(\alpha), y(\alpha)$, and $y^2(\alpha)$

We recall and introduce here some needed terminology.

Definition 2.1. (see [2])
1. An element $\alpha \in \mathbb{Q}^*(\sqrt{-n})$ is said to be *totally positive* (resp. *totally negative*) if $a_\alpha c_\alpha > 0$ (resp. $a_\alpha c_\alpha < 0$).
2. The ordered triple $(a_\alpha, b_\alpha, c_\alpha)$ is called *the signature of* $\alpha \in \mathbb{Q}^*(\sqrt{-n})$.
3. Define the map $\|.\| : \mathbb{Q}^*(\sqrt{-n}) \to \mathbb{N} \cup \{0\}$ by $\|\alpha\| = |a_\alpha|$. We call $\|\alpha\|$ *the norm of* α (not to be confused with the classical notion of norm).

Definition 2.2. For $\alpha \in \mathbb{Q}^*(\sqrt{-n})$, we call the set $\{\alpha, y(\alpha), y^2(\alpha)\}$ the α-cycle and denote it by $\widehat{\alpha}$. We say that $\widehat{\alpha}$ is a *totally positive cycle* if $\alpha, y(\alpha)$, and $y^2(\alpha)$ are all totally positive. We denote by $T^+(-n)$ the set of all totally positive cycles in $\mathbb{Q}^*(\sqrt{-n})$.

Remark 2.2.
1. For $\frac{a+\sqrt{-n}}{c} \in \mathbb{Q}^*(\sqrt{-n})$, $bc = a^2 + n$ is always positive. So, b and c always have the same sign. So, an equivalent useful definition to Definition 2.1 (part 1) can go like this: $\alpha \in \mathbb{Q}^*(\sqrt{-n})$ is said to be totally positive if either $a_\alpha, b_\alpha, c_\alpha > 0$ or $a_\alpha, b_\alpha, c_\alpha < 0$; and α is said to be totally negative if either ($a_\alpha < 0$ and $b_\alpha, c_\alpha > 0$) or ($a_\alpha > 0$ and $b_\alpha, c_\alpha < 0$). Note that any $\alpha \in \mathbb{Q}^*(\sqrt{-n})$ is either totally positive, totally negative, or has norm zero.
2. In Definition 2.2, note that $\widehat{\alpha} = \widehat{y(\alpha)} = \widehat{y^2(\alpha)}$, so we can equally call $\widehat{\alpha}$ the $y(\alpha)$-cycle or the $y^2(\alpha)$-cycle.

Example 2.1. For $n = 5$, $\alpha = \frac{1+\sqrt{-5}}{2} \in \mathbb{Q}^*(\sqrt{-5})$ is totally positive. From Table 1, we have $y(\alpha) = \frac{2+\sqrt{-5}}{3}$ and $y^2(\alpha) = \frac{1+\sqrt{-5}}{3}$. It is clear that $y(\alpha)$ and $y^2(\alpha)$ are both totally positive as well. So, $\widehat{\alpha} \in T^+(-5)$.

For $\alpha \in \mathbb{Q}^*(\sqrt{-n})$, denote the orbit $\{\beta \in \mathbb{Q}^*(\sqrt{-n}) \mid \beta = g(\alpha),\ g \in G\}$ by α^G. Denote the set of orbits in $\mathbb{Q}^*(\sqrt{-n})$ under the action of G by $\mathcal{O}^G(\mathbb{Q}^*(\sqrt{-n}))$; so $\mathcal{O}^G(\mathbb{Q}^*(\sqrt{-n})) := \{\alpha^G \mid \alpha \in \mathbb{Q}^*(\sqrt{-n})\}$. We adopt the standard notation $d(n)$ for the number of positive divisors of n. For two positive integers $k \leq m$, denote by $d_{\leq k}(m)$ the number of positive divisors of m which are less than or equal to k. For instance, $d_{\leq 4}(10) = 2$ and $d_{\leq 10}(10) = d(10) = 4$.

We state our main result, which gives a formula for the number of orbits $|\mathcal{O}^G(\mathbb{Q}^*(\sqrt{-n}))|$ and an interesting congruence property of such a number.

Theorem 2.1. *Let n be a square-free positive integer. Then the number of orbits in $\mathbb{Q}^*(\sqrt{-n})$ under the action of G is*

$$|\mathcal{O}^G(\mathbb{Q}^*(\sqrt{-n}))| = \begin{cases} 2 & , \textit{if } n = 1, 2 \\ 4 & , \textit{if } n = 3 \\ d(n) + \frac{2}{3} \sum_{i=1}^{\lfloor (n-1)/2 \rfloor} [d(i^2+n) - 2d_{\leq i}(i^2+n)] & , \textit{otherwise.} \end{cases}$$

Moreover, $|\mathcal{O}^G(\mathbb{Q}^*(\sqrt{-n}))| \equiv 0 \pmod 4$ *for* $n \geq 3$.

3. Lemmas and Proof of Theorem 2.1

3.1. Lemmas

In preparation for the proof of Theorem 2.1, we consider crucial lemmas, some of which are interesting in their own right.

The following lemma shows that the sign of the denominators of elements in any given orbit is the same.

Lemma 3.1. *For $\alpha \in \mathbb{Q}^*(\sqrt{-n})$, $sign(c_\beta) = sign(c_\alpha)$ for any $\beta \in \alpha^G$.*

Proof. It is sufficient to show that $c_{x(\alpha)}$ and $c_{y(\alpha)}$ have the same sign as c_α. By Remark 2.2, b_α and c_α have the same sign. Since $c_{x(\alpha)} = c_{y(\alpha)} = b_\alpha$ (Table 1), $c_{x(\alpha)}$ and $c_{y(\alpha)}$ have the same sign as c_α. □

The effect of the action of x on elements of $\mathbb{Q}^*(\sqrt{-n})$ and their norms is given below.

Lemma 3.2. *Let $\alpha \in \mathbb{Q}^*(\sqrt{-n})$. Then,*
1. *α is totally negative if and only if $x(\alpha)$ is totally positive.*
2. *$\|\alpha\| = \|x(\alpha)\|$. Further, α has norm zero if and only if $x(\alpha)$ has norm zero.*

Proof.
1. This follows from the fact that $b_\alpha c_\alpha > 0$, $a_{x(\alpha)} = -a_\alpha$, and $c_{x(\alpha)} = b_\alpha$; see Table 1 and Remark 2.2.
2. The first statement is clear from Table 1, while the second statement follows from the first. □

Some aspects of the actions of y and y^2 on elements of $\mathbb{Q}^*(\sqrt{-n})$ and their norms are given below.

Lemma 3.3. *Let $\alpha = \frac{a+\sqrt{-n}}{c} \in \mathbb{Q}^*(\sqrt{-n})$.*
1. *If α has norm zero, then $y(\alpha)$ and $y^2(\alpha)$ are both totally positive.*
2. *If α is totally negative, then $y(\alpha)$ and $y^2(\alpha)$ are both totally positive with $\|\alpha\| < \|y(\alpha)\|$ and $\|\alpha\| < \|y^2(\alpha)\|$.*
3. *The α-cycle $\widehat{\alpha}$ is totally positive if and only if either $(0 < a$, $a < b$, and $a < c)$ or $(0 > a$, $a > b$, and $a > c)$.*

Proof.
1. Since $a = 0$, it follows from Table 1 that $a_{y(\alpha)}c_{y(\alpha)} = b^2 > 0$ and so $y(\alpha)$ is totally positive. Similarly, $a_{y^2(\alpha)}c_{y^2(\alpha)} = c(b+c) = n + c^2 > 0$ and so $y^2(\alpha)$ is totally positive as well.
2. Since α is totally negative, we have $ac < 0$ and, by Remark 2.2, $ab < 0$. We then have, from Table 1, $a_{y(\alpha)}c_{y(\alpha)} = (b-a)b = b^2 - ab > 0$ and so $y(\alpha)$ is totally positive. Similarly, $a_{y^2(\alpha)}b_{y^2(\alpha)} = (c-a)c = c^2 - ac > 0$. Thus, by Remark 2.2, $a_{y^2(\alpha)}c_{y^2(\alpha)} > 0$ and so $y^2(\alpha)$ is totally positive as well. As for the norms in this case, we have $\|y(\alpha)\| = |b-a| = b-a > -a = \|\alpha\|$ and $\|y^2(\alpha)\| = |c-a| = c-a > -a = \|\alpha\|$.
3. Suppose that $\widehat{\alpha}$ is a totally positive cycle. Since α is totally positive, $a, b, c > 0$ or $a, b, c < 0$. Assume that $a, b, c > 0$. Since $c_{y(\alpha)} = b > 0$ and $y(\alpha)$ is totally positive, $a_{y(\alpha)} = b - a > 0$. So $b > a$ as desired. On the other hand, since $b_{y^2(\alpha)} = c > 0$ (and, hence, $c_{y^2(\alpha)} > 0$) and $y^2(\alpha)$ is totally positive, $a_{y^2(\alpha)} = c - a > 0$. So $c > a$ as desired. Similarly, if

$a, b, c < 0$, it follows that $a > b$ and $a > c$. Conversely, suppose that $0 < a$, $a < b$, and $a < c$. Since $ac > 0$, α is totally positive. As $a_{y(\alpha)} = b - a > 0$ and $c_{y(\alpha)} = b > 0$, $y(\alpha)$ is totally positive too. Also, as $a_{y^2(\alpha)} = c - a > 0$ and $b_{y^2(\alpha)} = c > 0$ (and, hence, $c_{y^2(\alpha)} > 0$), $y^2(\alpha)$ is totally positive as well. This shows that $\widehat{\alpha}$ is a totally positive cycle. A similar argument works if $0 > a$, $a > b$, and $a > c$. □

Remark 3.1. It is apparent from the above lemma that for any three elements $\alpha, y(\alpha), y^2(\alpha)$ of $\mathbb{Q}^*(\sqrt{-n})$, either all three are totally positive, one is totally negative and the other two are totally positive, or one is of norm zero and the other two are totally positive. This remark shall show to be useful shortly. In the terminology of coset diagrams (see [6], [7], or [11] for example), the triangle whose vertices are $\alpha, y(\alpha), y^2(\alpha)$ always has one of three properties: either all vertices are totally positive, one vertex is totally negative and the other two are totally positive, or one vertex is of norm zero and the other two are totally positive. We chose, however, to not use the machinery of coset diagrams in this paper as combinatorial arguments suffice.

Lemma 3.4. *Under the action of G, every orbit in $\mathbb{Q}^*(\sqrt{-n})$ contains both a totally negative element and a totally positive element.*

Proof. Consider an orbit α^G for some $\alpha \in \mathbb{Q}^*(\sqrt{-n})$. By Remark 2.2 (part 1), α is either totally negative, totally positive, or has norm zero. By Lemma 3.2, if α is totally negative, then $x(\alpha)$ is totally positive, and conversely. Finally, if α is of norm zero, then $y(\alpha)$ is totally positive by Lemma 3.3 and so $xy(\alpha)$ is totally negative. □

The following lemma specifies the elements of $\mathbb{C}$ fixed by x or y.

Lemma 3.5. *Under the action of G on $\mathbb{C}$, the only complex numbers fixed by x are $\pm i \in \mathbb{Q}^*(\sqrt{-1})$ and the only numbers fixed by y are $\frac{1\pm\sqrt{-3}}{2} \in \mathbb{Q}^*(\sqrt{-3})$.*

Proof. Let $z \in \mathbb{C}$ be such that $x(z) = z$. Then $z^2 = -1$, which implies that $z = \pm i$. If $y(z) = z$, then $z^2 - z + 1 = 0$, which implies that $z = \frac{1\pm\sqrt{-3}}{2}$. □

Remark 3.2. The latter statement in Lemma 3.5 entails that every α-cycle in $\mathbb{Q}^*(\sqrt{-n})$ consists of 3 distinct elements except when $n = 3$ and α is $\frac{1+\sqrt{-3}}{2}$ or $\frac{-1+\sqrt{-3}}{-2}$, in which cases the α-cycle is a singleton.

From Definition 2.2, recall that

$$T^+(-n) := \left\{\widehat{\alpha} \mid \alpha \in \mathbb{Q}^*(\sqrt{-n}) \text{ and } \widehat{\alpha} \text{ is a totally positive cycle}\right\}.$$

According to Definition 2.1 (part 2), consider the two sets of signatures of totally positive elements of $\mathbb{Q}^*(\sqrt{-n})$ (by Lemma 3.3):

$$A^+(-n) := \left\{(a, b, c) \in \mathbb{Z}^3 \mid a > 0,\, b = \frac{a^2 + n}{c} > a,\, c > a\right\},$$

$$A^-(-n) := \left\{(a, b, c) \in \mathbb{Z}^3 \mid a < 0,\, b = \frac{a^2 + n}{c} < a,\, c < a\right\}.$$

It is clear that $\frac{a+\sqrt{-n}}{c} \in \mathbb{Q}^*(\sqrt{-n})$ for every $(a, b, c) \in A^+(-n) \cup A^-(-n)$.

Next, we use the action of the cyclic subgroup G_y of G generated by y on $\mathbb{Q}^*(\sqrt{-n})$ induced from the action of G to define an action of G_y on $A^+(-n)$ when $A^+(-n)$ is nonempty. Considering the signature in $A^+(-n)$ of some $\alpha \in \mathbb{Q}^*(\sqrt{-n})$, it is obvious that such a desired action of y on $A^+(-n)$ is to map the signature of α to the signature of $y(\alpha)$. Namely, define the map $G_y \times A^+(-n) \to A^+(-n)$, denoted by $g \cdot (a,b,c)$ for $g \in G_y$ and $(a,b,c) \in A^+(-n)$, by $1 \cdot (a,b,c) = (a,b,c)$, $y \cdot (a,b,c) = (b-a, -2a+b+c, b)$ and $y^2 \cdot (a,b,c) = y \cdot (y \cdot (a,b,c)) = (c-a, c, -2a+b+c)$, see Table 1. To show that this is indeed a map into $A^+(-n)$, it suffices to show that $y \cdot (a,b,c) \in A^+(-n)$ for $(a,b,c) \in A^+(-n)$. We have $0 < a$, $a < b$, and $a < c$. So, $0 < b-a = a_{y(\alpha)}$, $a_{y(\alpha)} = b-a < b-a+c-a = b_{y(\alpha)}$ and $a_{y(\alpha)} = b-a < b = c_{y(\alpha)}$, from which is follows that $y \cdot (a,b,c) \in A^+(-n)$ as desired. Now, by the way we defined this map, it is obvious that it satisfies the axioms of a group action. Hence, $A^+(-n)$ is a G_y-set under this induced action. Due to the symmetry between $A^+(-n)$ and $A^-(-n)$, the action of G_y on $A^-(-n)$ is defined similarly. Indeed, we have just proved the following Lemma.

Lemma 3.6. *If $A^+(-n)$ and $A^-(-n)$ are non-empty, then $A^+(-n)$ and $A^-(-n)$ are G_y-sets under the induced action defined in the above paragraph.*

The following two lemmas show, in particular, that the sets $A^+(-n)$ and $T^+(-n)$ are finite and give a formula that compares their respective cardinalities for $n \neq 3$.

Lemma 3.7. *We have that $A^+(-1) = A^+(-2) = \varnothing$. If $n \geq 3$ and $(a,b,c) \in A^+(-n)$, then $a \leq \frac{n-1}{2}$ and $b, c \leq \frac{n+1}{2}$. Furthermore, $|A^+(-n)| \leq \frac{n^2-1}{8}$.*

Proof. Let $(a,b,c) \in A^+(-n)$. Since $a+1 \leq b$ and $a+1 \leq c$, we have $a^2+2a+1 = (a+1)^2 \leq bc = a^2+n$, from which it follows that $a \leq \frac{n-1}{2}$. If $n \leq 2$, this leads to a contradiction, therefore $A^+(-1) = A^+(-2) = \varnothing$. For $n \geq 3$, consider $f : [1, \frac{n-1}{2}] \to \mathbb{R}$ defined by $f(x) = \frac{x^2+n}{x+1}$. From the sign of f', it follows that f is decreasing on $[1, -1+\sqrt{n+1}]$ and increasing on $[-1+\sqrt{n+1}, \frac{n-1}{2}]$. On the other hand, $f(1) = f(\frac{n-1}{2}) = \frac{n+1}{2}$. Hence, $b \leq \frac{a^2+n}{a+1} = f(a) \leq \frac{n+1}{2}$. Now, an element $(a,b,c) \in A^+(-n)$ is determined by a choice of a and b (as $c = \frac{a^2+n}{b}$) with $1 \leq a < b \leq \frac{n+1}{2}$. Since the number of such pairs (a,b) is $\binom{\frac{n+1}{2}}{2}$, we have $|A^+(-n)| \leq \frac{1}{2}\left(\frac{n+1}{2}\right)\left(\frac{n+1}{2}-1\right) = \frac{n^2-1}{8}$. □

Lemma 3.8.
1. $|A^+(-1)| = |A^+(-2)| = 0$.
2. $|A^+(-n)| = 1$ *if and only if* $n = 3$.
3. $|A^+(-n)| \equiv 0 \pmod 3$ *for* $n \neq 3$.
4. $|T^+(-n)| = \frac{2}{3}|A^+(-n)|$ *for* $n \neq 3$

Proof.
1. It is obvious from Lemma 3.7.
2. Since $(1,2,2) \in A^+(-3)$ and $|A^+(-3)| \leq \frac{3^2-1}{8} = 1$, we get $|A^+(-3)| = 1$.
3. Let $n \neq 3$. If $A^+(-n) = \varnothing$, then $|A^+(-n)| = 0$ and we are done. Suppose that $(a,b,c) \in A^+(-n)$ and α is the element of $\mathbb{Q}^*(\sqrt{-n})$ whose signature is (a,b,c). Since the set $A^+(-n)$ is finite (by Lemma 3.7), the number of orbits in $A^+(-n)$ under the action of G_y (Lemma 3.6) is finite as well. Considering the action of G_y on $\mathbb{Q}^*(\sqrt{-n})$ induced from the action of G, we see that the totally positive α-cycle $\widehat{\alpha}$ is G_y-invariant and so is the corresponding set of signatures $\{(a,b,c), (b-a, -2a+b+c, b), (c-a, c, -2a+b+c)\}$ in $A^+(-n)$. Since $n \neq 3$, the elements of the set $\widehat{\alpha}$ are distinct and so are the elements of the corresponding set of signatures $\{(a,b,c), (b-a, -2a+b+c, b), (c-a, c, -2a+b+c)\}$.

This means that each orbit in $A^+(-n)$, under the action of G_y, consists precisely of three elements and, hence, $|A^+(-n)|$ is divisible by 3 as claimed.
4. Let $n \neq 3$. It is clear that the two sets $A^+(-n)$ and $A^-(-n)$ are disjoint and that there is a bijection between them. It can also be easily seen that the same arguments in parts 1, 2, and 3 above apply also to $A^-(-n)$. Let $\mathcal{O}^{G_y}(A^+(-n))$ and $\mathcal{O}^{G_y}(A^-(-n))$ be the sets of orbits in $A^+(-n)$ and $A^-(-n)$, respectively, under the action of G_y. It follows from the argument in the proof of Lemma 3.6 and part 3 above that there is the bijection from $T^+(-n)$ into the disjoint union $\mathcal{O}^{G_y}(A^+(-n)) \cup \mathcal{O}^{G_y}(A^-(-n))$ given by

$$\widehat{\alpha} \mapsto \{(a,b,c),(b-a,-2a+b+c,b),(c-a,c,-2a+b+c)\}.$$

Since we have, by part 3 above,

$$|\mathcal{O}^{G_y}(A^+(-n))| = (1/3)\,|A^+(-n)| = (1/3)\,|A^-(-n)| = |\mathcal{O}^{G_y}(A^-(-n))|$$

and the two sets of orbits are disjoint, we get $|T^+(-n)| = \frac{2}{3}\,|A^+(-n)|$. □

Lemma 3.9. *The number of elements of norm zero in $\mathbb{Q}^*(\sqrt{-n})$ is equal to $2d(n)$.*

Proof. For $\alpha = \frac{\sqrt{-n}}{c_\alpha} \in \mathbb{Q}^*(\sqrt{-n})$, $b_\alpha = \frac{n}{c_\alpha} \in \mathbb{Z}$ if and only if c_α is a divisor of n. Considering positive and negative divisors of n, the conclusion follows. □

The last round in our effort to prove Theorem 2.1 is Corollary 3.1 below. For this, we need the following two lemmas.

Lemma 3.10.
1. *Every orbit in $\mathbb{Q}^*(\sqrt{-n})$ contains at most one element of $T^+(-n)$.*
2. *Every orbit in $\mathbb{Q}^*(\sqrt{-n})$ contains at most two elements of norm zero.*

Proof.
1. Suppose that $\widehat{\alpha} \in T^+(-n)$ for some $\alpha \in \mathbb{Q}^*(\sqrt{-n})$. Let $\beta \in \alpha^G \setminus \widehat{\alpha}$. We show that $\widehat{\beta} \notin T^+(-n)$ by showing that the β-cycle $\widehat{\beta}$ must contain a totally negative element. Since the action of G on the orbit α^G is transitive and $\widehat{\alpha} \neq \widehat{\beta}$, there is some $g \in G \setminus \{1, y, y^2\}$ such that $g(\alpha) = \beta$. Since x and y are of order 2 and 3, respectively, it can be checked that g is of one of the following forms:

$$\begin{aligned}
&g_1 = x,\\
&g_2 = xy^{\varepsilon_1}xy^{\varepsilon_2}x\ldots xy^{\varepsilon_k}, \quad k \geq 1,\, \varepsilon_i = 1 \text{ or } 2,\, i = 1,\ldots,k,\\
&g_3 = xy^{\varepsilon_1}xy^{\varepsilon_2}x\ldots xy^{\varepsilon_k}x, \quad k \geq 1,\, \varepsilon_i = 1 \text{ or } 2,\, i = 1,\ldots,k,\\
&g_4 = y^{\varepsilon_1}xy^{\varepsilon_2}x\ldots xy^{\varepsilon_k}, \quad k \geq 1,\, \varepsilon_i = 1 \text{ or } 2,\, i = 1,\ldots,k,\\
&g_5 = y^{\varepsilon_1}xy^{\varepsilon_2}x\ldots xy^{\varepsilon_k}x, \quad k \geq 1,\, \varepsilon_i = 1 \text{ or } 2,\, i = 1,\ldots,k.
\end{aligned}$$

If $g = g_1$, then $\beta = x(\alpha)$ is totally negative (since α is totally positive), by Lemma 3.2. So $\widehat{\beta} \notin T^+(-n)$. Assume that $g = g_2$. As $y^{\varepsilon_k}(\alpha) \in \widehat{\alpha}$, it follows that $y^{\varepsilon_k}(\alpha)$ is totally positive and so $xy^{\varepsilon_k}(\alpha)$ is totally negative, by Lemma 3.2. Then, by Lemma 3.3, $y^{\varepsilon_{k-1}}xy^{\varepsilon_k}(\alpha)$ is totally positive. Continuing in this manner by applying x to $y^{\varepsilon_{k-1}}xy^{\varepsilon_k}(\alpha)$ then applying $y^{\varepsilon_{k-2}}$ and so on, we get that $\gamma = y^{\varepsilon_1}xy^{\varepsilon_2}x\ldots xy^{\varepsilon_k}(\alpha)$ is totally positive. Thus, $\beta = g_2(\alpha) = x(\gamma)$ is totally negative and so $\widehat{\beta} \notin T^+(-n)$. The case $g = g_3$ is similar to the case $g = g_2$ starting with $y^{\varepsilon_k}x(\alpha)$ being totally positive instead of $y^{\varepsilon_k}(\alpha)$. Now, if $g = g_4$, we follow the same argument to get that $\delta = xy^{\varepsilon_2}x\ldots xy^{\varepsilon_k}(\alpha)$ is totally negative. Since $\beta = g_4(\alpha) = y^{\varepsilon_1}(\delta)$,

$\widehat{\beta} = \widehat{\delta}$ (see Remark 2.2 (2)). So, $\widehat{\beta} \notin T^+(-n)$ since $\delta \in \widehat{\beta}$ and δ is totally negative. The case $g = g_5$ is similar to the case $g = g_4$. By this, we showed in all cases that $\widehat{\beta} \notin T^+(-n)$ and so $\widehat{\alpha}$ is the only element of $T^+(-n)$ lying in the orbit α^G.

2. Let α be of norm zero. Then, $x(\alpha)$ is also of norm zero (Lemma 3.2). Let $\beta \in \alpha^G \setminus \{\alpha, x(\alpha)\}$. We show that β must be either totally negative or totally positive and so can never be of norm zero. By the transitivity of the action of G on α^G, let $h \in G$ be such that $h(\beta) = \alpha$. It can be checked that h is of one of the following forms:

$$\begin{aligned}
&h_1 = y^{\varepsilon}, \quad \varepsilon = 1 \text{ or } 2,\\
&h_2 = xy^{\varepsilon_1}xy^{\varepsilon_2}x \dots xy^{\varepsilon_k}, \quad k \geq 1,\, \varepsilon_i = 1 \text{ or } 2,\, i = 1, \dots, k,\\
&h_3 = xy^{\varepsilon_1}xy^{\varepsilon_2}x \dots xy^{\varepsilon_k}x, \quad k \geq 1,\, \varepsilon_i = 1 \text{ or } 2,\, i = 1, \dots, k,\\
&h_4 = y^{\varepsilon_1}xy^{\varepsilon_2}x \dots xy^{\varepsilon_k}, \quad k \geq 1,\, \varepsilon_i = 1 \text{ or } 2,\, i = 1, \dots, k,\\
&h_5 = y^{\varepsilon_1}xy^{\varepsilon_2}x \dots xy^{\varepsilon_k}x, \quad k \geq 1,\, \varepsilon_i = 1 \text{ or } 2,\, i = 1, \dots, k.
\end{aligned}$$

If $h = h_1$, then $\beta = y^{\varepsilon}(\alpha)$ is totally positive (Lemma 3.3). Assume that $h = h_2$, then $y^{\varepsilon_k}(\alpha)$ is totally positive (Lemma 3.3) and so $xy^{\varepsilon_k}(\alpha)$ is totally negative (Lemma 3.2). Applying $y^{\varepsilon_{k-1}}$ to $xy^{\varepsilon_k}(\alpha)$ followed by x, then $y^{\varepsilon_{k-2}}$ followed by x and so on, we get that $\beta = h_2(\alpha)$ is totally negative. In a similar manner, we get that $h_3(\alpha)$ is totally negative, $h_4(\alpha)$ is totally positive, and $h_5(\alpha)$ is totally positive. This shows that β is never of norm zero. □

Lemma 3.11. *Every orbit in $\mathbb{Q}^*(\sqrt{-n})$ contains either an element of $T^+(-n)$ or an element of norm zero, but not both.*

Proof. Let α^G be an orbit in $\mathbb{Q}^*(\sqrt{-n})$. On the one hand, suppose that α^G contains some $\widehat{\beta} \in T^+(-n)$. It remains, in this direction, to show that α^G contains no element of norm zero. Obviously, no element in $\widehat{\beta}$ is of norm zero. It also follows from the argument in the proof of Lemma 3.10 (part 1) that for any $\gamma \in \alpha^G \setminus \widehat{\beta}$, one of the elements of $\widehat{\gamma} = \{\gamma, y(\gamma), y^2(\gamma)\}$ is totally negative. Now, as an easy consequence of Lemma 3.3, γ cannot be of norm zero (as, otherwise, $\widehat{\gamma}$ would not have a totally negative element).

On the other hand, suppose that α^G contains no element of $T^+(-n)$. We show that α^G must contain an element of norm zero. By Lemma 3.4, let $\alpha_1 \in \alpha^G$ be a totally negative element and so $x(\alpha_1)$ is totally positive (Lemma 3.2). If the cycle $\widehat{x(\alpha_1)}$ contains an element of norm zero, then we are done. Otherwise, since $\widehat{x(\alpha_1)} \notin T^+(-n)$ and $x(\alpha_1)$ is totally positive, $\widehat{x(\alpha_1)}$ contains a totally negative element $\alpha_2 = y^{\varepsilon_1}x(\alpha_1)$ with $\varepsilon_1 = 1$ or 2. Moreover, by Lemmas 3.2 and 3.3,

$$\|\alpha_2\| < \|y^{3-\varepsilon_1}(\alpha_2)\| = \|x(\alpha_1)\| = \|\alpha_1\|.$$

Now, if $\widehat{x(\alpha_2)}$ contains an element of norm zero, then we are done. Otherwise, since $\widehat{x(\alpha_2)} \notin T^+(-n)$ and $x(\alpha_2)$ is totally positive, $\widehat{x(\alpha_2)}$ contains a totally negative element $\alpha_3 = y^{\varepsilon_2}x(\alpha_2)$ with $\varepsilon_2 = 1$ or 2. Moreover, an argument similar to the one above yields the inequality $\|\alpha_3\| < \|\alpha_2\|$. Suppose that this process of getting totally negative elements in α^G never terminates (i.e. the process never yields an element of norm zero). Then, we would have a sequence $\alpha_1, \alpha_2, \alpha_3, \dots$ of totally negative elements in the orbit α^G with strictly decreasing norms

$$\|\alpha_1\| > \|\alpha_2\| > \|\alpha_3\| > \dots$$

However, the latter sequence of norms is a strictly decreasing sequence of positive integers which obviously must terminate. This contradicts the non-termination of the sequence of totally negative elements $\alpha_1, \alpha_2, \alpha_3, \dots$, which in turn proves that α^G has to contain an element of norm zero. □

Corollary 3.1.
1. *Every orbit in* $\mathbb{Q}^*(\sqrt{-1})$ *contains a unique element of norm zero.*
2. *Every orbit in* $\mathbb{Q}^*(\sqrt{-2})$ *contains a unique pair of distinct elements of norm zero.*
3. *Every orbit in* $\mathbb{Q}^*(\sqrt{-n})$*, for* $n \geq 3$*, contains either a unique pair of distinct elements of norm zero or a unique element of* $T^+(-n)$*, but not both. In this case, we have* $|\mathcal{O}^G(\mathbb{Q}^*(\sqrt{-n}))| = d(n) + |T^+(-n)|$.

Proof.
1. By Lemma 3.8, $T^+(-1) = \varnothing$. So, every orbit in $\mathbb{Q}^*(\sqrt{-1})$ contains an element of norm zero, by Lemma 3.11. Since the only elements of norm zero in $\mathbb{Q}^*(\sqrt{-1})$ are i and $-i$ (Lemma 3.9) and they lie in distinct orbits (Lemma 3.1), the conclusion follows.
2. By Lemma 3.8, $T^+(-2) = \varnothing$. So, every orbit in $\mathbb{Q}^*(\sqrt{-2})$ contains an element of norm zero, by Lemma 3.11. By Lemma 3.9, there are precisely 4 elements of norm zero in $\mathbb{Q}^*(\sqrt{-2})$; namely $\sqrt{-2}$, $-\sqrt{-2}$, $\frac{\sqrt{-2}}{2}$ and $\frac{-\sqrt{-2}}{2}$. Note further that $\frac{\sqrt{-2}}{2} = x(\sqrt{-2})$ and $\frac{-\sqrt{-2}}{2} = x(-\sqrt{-2})$. Now, by Lemma 3.1, the two pairs $\left(\sqrt{-2}, \frac{\sqrt{-2}}{2}\right)$ and $\left(-\sqrt{-2}, \frac{-\sqrt{-2}}{2}\right)$ lie in distinct orbits. The conclusion now follows.
3. For $n \geq 3$, it follows from Corollary 3.1 (part 3) that the orbits in $\mathbb{Q}^*(\sqrt{-n})$ are precisely of two types. There are those orbits each of which contains a unique element of $T^+(-n)$ and contains no zero-norm elements, and there are those orbits each of which contains a unique pair of distinct zero-norm elements and contains no elements of $T^+(-n)$. Thus, the total number of orbits in $\mathbb{Q}^*(\sqrt{-n})$ is equal to $|T^+(-n)|$ plus half the number of zero-norm elements in $\mathbb{Q}^*(\sqrt{-n})$. So, by Lemma 3.9, the claimed formula for the total number of orbits follows. □

3.2. Proof of Theorem 2.1

Proof. (**Theorem 2.1**)

For $n = 1$ and $n = 2$, it follows from Corollary 3.1 (parts 1 and 2) and their proofs that $|\mathcal{O}^G(\mathbb{Q}^*(\sqrt{-1}))| = |\mathcal{O}^G(\mathbb{Q}^*(\sqrt{-2}))| = 2$.

For $n = 3$, it follows from Lemma 3.5 and the argument in the proof of Lemma 3.8 (part 2) that $T^+(-3) = \left\{\left\{\frac{1+\sqrt{-3}}{2}\right\}, \left\{\frac{-1+\sqrt{-3}}{-2}\right\}\right\}$. Thus, by Corollary 3.1 (part 3), $|\mathcal{O}^G(\mathbb{Q}^*(\sqrt{-3}))| = d(3) + |T^+(-3)| = 2 + 2 = 4$.

For $n > 3$, it follows from Corollary 3.1 (part 3) and Lemma 3.8 that

$$|\mathcal{O}^G(\mathbb{Q}^*(\sqrt{-n}))| = d(n) + |T^+(-n)| = d(n) + \frac{2}{3}\,|A^+(-n)|. \tag{1}$$

So the desired claim in this case holds if and only if

$$|A^+(-n)| = \sum_{i=1}^{\lfloor \frac{n-1}{2} \rfloor} [d(i^2+n) - 2d_{\leq i}(i^2+n)].$$

We seek now to prove this last equality. Making use of Lemma 3.7, we first write the set $A^+(-n)$ as a disjoint union of subsets in the form

$$A^+(-n) = A_1^+(-n) \cup A_2^+(-n) \cup \cdots \cup A^+_{\lfloor \frac{n-1}{2} \rfloor}(-n),$$

where, for each $i = 1, 2, \ldots, \lfloor \frac{n-1}{2} \rfloor$,

$$A_i^+(-n) := \left\{ (i, b, c) \in \mathbb{Z}^3 \mid i > 0,\, b = \frac{i^2+n}{c} > i,\, c > i \right\}.$$

For a fixed such i, we can see that $A_i^+(-n) = A^+_{i,d_1}(-n) - \left\{ A^+_{i,d_2}(-n) \cup A^+_{i,d_3}(-n) \right\}$, where

$$A^+_{i,d_1}(-n) := \left\{ (i, d_1, \frac{i^2+n}{d_1}) \in A_i^+(-n) \mid d_1 | (i^2+n) \right\},$$
$$A^+_{i,d_2}(-n) := \left\{ (i, d_2, \frac{i^2+n}{d_2}) \in A_i^+(-n) \mid d_2 \le i,\ d_2 | (i^2+n) \right\},$$
$$A^+_{i,d_3}(-n) := \left\{ (i, \frac{i^2+n}{d_3}, d_3) \in A_i^+(-n) \mid d_3 \le i,\ d_3 | (i^2+n) \right\}.$$

Note that $|A^+_{i,d_1}(-n)| = d(i^2+n)$ and $|A^+_{i,d_2}(-n)| = |A^+_{i,d_3}(-n)| = d_{\le i}(i^2+n)$. If the latter two sets have a point in common, then for some $d_2 \le i$ and $d_3 \le i$ we would have $d_2 d_3 = i^2 + n \le i^2$, which is absurd. So, these two sets are disjoint and, hence,

$$|A_i^+(-n)| = |A^+_{i,d_1}(-n)| - |A^+_{i,d_2}(-n)| - |A^+_{i,d_3}(-n)| = d(i^2+n) - 2d_{\le i}(i^2+n).$$

As $|A^+(-n)| = |A_1^+(-n)| + |A_2^+(-n)| + \cdots + |A^+_{\lfloor \frac{n-1}{2} \rfloor}(-n)|$, the desired equality follows.

We now prove that $|\mathcal{O}^G(\mathbb{Q}^*(\sqrt{-n}))| \equiv 0 \pmod{4}$ for $n \ne 1$ or 2. Since $|\mathcal{O}^G(\mathbb{Q}^*(\sqrt{-3}))| = 4$, $|\mathcal{O}^G(\mathbb{Q}^*(\sqrt{-3}))| \equiv 0 \pmod{4}$. Let $n > 3$. Then, by (1), $|\mathcal{O}^G(\mathbb{Q}^*(\sqrt{-n}))| = d(n) + \frac{2}{3}\,|A^+(-n)|$. It thus follows that

$$|\mathcal{O}^G(\mathbb{Q}^*(\sqrt{-n}))| \equiv d(n) + 2\,|A^+(-n)| \pmod{4}.$$

We write the set $A^+(-n)$ as the disjoint union of subsets in the form

$$A^+(-n) = A^+_{b \ne c}(-n) \cup A^+_{b=c}(-n),$$

where

$$A^+_{b \ne c}(-n) := \{(a,b,c) \in A^+(-n) \mid b \ne c\}$$

and

$$A^+_{b=c}(-n) := \{(a,b,c) \in A^+(-n) \mid b = c\}.$$

By Lemma 3.7, the two sets $A^+_{b\ne c}(-n)$, and $A^+_{b=c}(-n)$ are finite. As a general observation, we can see that $(a,b,c) \in A^+(-n)$ if and only if $(a,c,b) \in A^+(-n)$, which implies that elements in the set $A^+_{b\ne c}(-n)$ occur in pairs. Thus, $|A^+_{b\ne c}(-n)|$ is always even. For the rest of the proof, we deal with three cases separately: when n is an even composite integer, when n is an odd prime, and when n is an odd composite integer.

Case 1: Let n be an even composite integer with $n = 2m$ for some $m > 1$ with m odd (as n is square-free). Since $d(n) = d(2)d(m) = 2d(m)$ and $2|d(m)$, $d(n) \equiv 0 \pmod{4}$. So, $|\mathcal{O}^G(\mathbb{Q}^*(\sqrt{-n}))| \equiv 2|A^+(-n)| \pmod{4}$. Since $|A^+(-n)| = |A^+_{b\ne c}(-n)| + |A^+_{b=c}(-n)|$ and $|A^+_{b\ne c}(-n)|$ is even, $|\mathcal{O}^G(\mathbb{Q}^*(\sqrt{-n}))| \equiv 2|A^+_{b=c}(-n)| \pmod{4}$ in this case. Let $(a,b,b) \in A^+_{b=c}(-n)$. Then $b^2 = a^2 + n$, which implies that $(b+a)(b-a) = n = 2m$. If $2|(b+a)$, then $b - a = \frac{m}{k}$, where $b + a = 2k$ and k is odd (as m is odd). Thus, $2b = 2k + \frac{m}{k}$ is odd, which is impossible. A similar contradiction occurs if $2|(b-a)$. We thus conclude that $A^+_{b=c}(-n)=\varnothing$ in this case and, hence, $|\mathcal{O}^G(\mathbb{Q}^*(\sqrt{-n}))|\equiv 0 \pmod 4$.

<u>Case 2:</u> Let n be an odd prime. So, $d(n)=2$ and so $d(n)\equiv 2 \ (\bmod\ 4)$. Then, $|\mathcal{O}^G(\mathbb{Q}^*(\sqrt{-n}))| \equiv 2+2\,|A^+(-n)| \pmod 4$ and, therefore, it suffices to show that $|A^+(-n)|$ is odd in this case. Since $|A^+(-n)|=|A^+_{b\neq c}(-n)|+|A^+_{b=c}(-n)|$ and $|A^+_{b\neq c}(-n)|$ is even, we show that $|A^+_{b=c}(-n)|$ is odd. We, in fact, show that $|A^+_{b=c}(-n)|=1$. For $(a,b,b)\in A^+_{b=c}(-n)$, $b^2=a^2+n$ and, thus, $(b+a)(b-a)=n$. Since $b+a>b-a$ and n is prime, we must have $b+a=n$ and $b-a=1$. Thus, $b=\frac{n+1}{2}$ and $a=\frac{n-1}{2}$. That is, $\left(\frac{n-1}{2},\frac{n+1}{2},\frac{n+1}{2}\right)$ is the only element in $A^+_{b=c}(-n)$. Hence, the claimed congruence is settled in this case too.

<u>Case 3:</u> Let n be an odd composite integer with $n=p_1p_2\dots p_r$, $r\geq 2$, where the p_i are distinct primes (as n is square-free). It then follows that $d(n)=\prod_{i=1}^r d(p_i)=2^r\equiv 0 \pmod 4$. So, $|\mathcal{O}^G(\mathbb{Q}^*(\sqrt{-n}))|\equiv 2\,|A^+(-n)| \pmod 4$ and, therefore, it suffices to show that $|A^+(-n)|$ is even in this case. Since $|A^+(-n)|=|A^+_{b\neq c}(-n)|$ $+|A^+_{b=c}(-n)|$ and $|A^+_{b\neq c}(-n)|$ is even, we show that $|A^+_{b=c}(-n)|$ is even as well. In fact, we prove the following stronger claim:

$$|A^+_{b=c}(-n)|=\begin{cases}\binom{r}{0}+\binom{r}{1}+\cdots+\binom{r}{\frac{r}{2}-1}_{r}+\frac{1}{2}\binom{r}{\frac{r}{2}} & ;\quad \text{if } r \text{ is even}\\ \binom{r}{0}+\binom{r}{1}+\cdots+\binom{r}{\frac{r-1}{2}-1}+\binom{r}{\frac{r-1}{2}} & ;\quad \text{if } r \text{ is odd,}\end{cases}$$

where $\binom{r}{k}$ are the binomial coefficients. For $(a,b,b)\in A^+_{b=c}(-n)$, we have $b^2=a^2+n$ and, thus, $(b+a)(b-a)=n=p_1p_2\dots p_r$. We notice that $b+a>b-a$ and investigate all the possible ways of factoring $b+a$ and $b-a$. Suppose that r is even. Then, there is $\binom{r}{0}=1$ way to write $b+a$ as the product of r primes (i.e. $b+a=n$) and $b-a$ is the product of no primes (i.e. $b-a=1$), and there is $\binom{r}{1}$ possibilities that $b+a$ is the product of $r-1$ primes and $b-a$ is the product of one prime. We continue in this manner until we get to the final scenario, which is where there are $\frac{1}{2}\binom{r}{\frac{r}{2}}$ ways of writing both of $b+a$ and $b-a$ as a product of $\frac{r}{2}$ primes each. Seeing obviously that each single possibility among the above ways of factorizations of $b+a$ and $b-a$ corresponds uniquely to a single point of $A^+_{b=c}(-n)$, the conclusion of the claim when r is even follows immediately. The case when r is odd is handled similarly. From elementary combinatorics (see [10] for instance), we know that $\sum_{k=0}^r\binom{r}{k}=2^r$ and $\binom{r}{k}=\binom{r}{r-k}$ for $k=0,\dots,r$. If r is even, then $\binom{r}{0}+\binom{r}{1}+\cdots+\binom{r}{\frac{r}{2}-1}+\frac{1}{2}\binom{r}{\frac{r}{2}}=\frac{1}{2}\binom{r}{\frac{r}{2}}+\binom{r}{\frac{r}{2}+1}+\cdots+\binom{r}{r}$. Thus, $2^r=\sum_{k=0}^r\binom{r}{k}=2\left(\binom{r}{0}+\binom{r}{1}+\cdots+\binom{r}{\frac{r}{2}-1}+\frac{1}{2}\binom{r}{\frac{r}{2}}\right)=2|A^+_{b=c}(-n)|$. Hence, $|A^+_{b=c}(-n)|=2^{r-1}$ which is even, as desired. The same conclusion is reached similarly if r is odd. This concludes the proof. □

Corollary 3.2. *The action of G on $\mathbb{Q}^*(\sqrt{-n})$ is intransitive.*

Proof. We have, by Theorem 2.1, $|\mathcal{O}^G(\mathbb{Q}^*(\sqrt{-1}))|=|\mathcal{O}^G(\mathbb{Q}^*(\sqrt{-2}))|=2$, $|\mathcal{O}^G(\mathbb{Q}^*(\sqrt{-3}))|=4$, and $|\mathcal{O}^G(\mathbb{Q}^*(\sqrt{-n}))|\geq d(n)\geq 2$ for $n>3$. The conclusion thus follows. □

Example 3.1. As an illustration, we compute in this example the value $|\mathcal{O}^G(\mathbb{Q}^*(\sqrt{-n}))|$ for $n=11$ in such a way that verifies Theorem 2.1 in this case. By Corollary 3.1 and Lemma 3.8, $|\mathcal{O}^G(\mathbb{Q}^*(\sqrt{-11}))|=d(11)+|T^+(-11)|=d(11)+\frac{2}{3}\ |A^+(-11)|$. Of course, $d(11)=2$. So, it remains to find $|A^+(-11)|$. By Lemma 3.7, for $(a,b,c)\in A^+(-11)$, $a\leq 5$ and $c\leq 6$. We try these values one by one. For $a=1$, $\frac{1^2+11}{c}\in\mathbb{Z}$ if and only if $c|12$. So, by Lemma 3.7 again, the possible candidate values of c are $1,2,3,4$, and 6. Since $a<c$, we discard the value $c=1$. For $c=2$, we have $b=6$ and we get that $(1,2,6)\in A^+(-11)$. For $c=3$,

we have $b = 4$ and we get that $(1, 3, 4) \in A^+(-11)$. For $c = 4$, we have $b = 3$ and we get that $(1, 4, 3) \in A^+(-11)$. For $c = 6$, we have $b = 2$ and we get that $(1, 6, 2) \in A^+(-11)$. For $a = 2$, $\frac{2^2+11}{c} \in \mathbb{Z}$ if and only if $c|15$. By an argument similar to the above, we get in this case only two elements $(2, 3, 5), (2, 5, 3) \in A^+(-11)$. For $a = 3$, $\frac{3^2+11}{c} \in \mathbb{Z}$ if and only if $c|20$. We also get in this case only two elements $(3, 4, 5), (3, 5, 4) \in A^+(-11)$. For $a = 4$, $\frac{4^2+11}{c} \in \mathbb{Z}$ if and only if $c|27$. The values $c = 1$ and 3 are discarded as $a < c$. Thus, for $a = 4$ we get no element in $A^+(-11)$. For $a = 5$, it can be checked similarly that we only get only the element $(5, 6, 6) \in A^+(-11)$. In summary, we have $|A^+(-11)| = 9$ and, thus, $|\mathcal{O}^G(\mathbb{Q}^*(\sqrt{-11}))| = d(11) + \frac{2}{3}\,(9) = 8$.

On the other hand, by Theorem 2.1, we have

$$\begin{aligned}
|\mathcal{O}^G(M_{-11})| &= d(11) + \frac{2}{3}\sum_{i=1}^{5}[d(i^2+11) - 2d_{\leq i}(i^2+11)] \\
&= 2 + \frac{2}{3}\,\{\,[d(12) + d(15) + d(20) + d(27) + d(36)] \\
&\quad - 2\,[d_{\leq 1}(12) + d_{\leq 2}(15) + d_{\leq 3}(20) + d_{\leq 4}(27) + d_{\leq 5}(36)]\,\} \\
&= 2 + \frac{2}{3}\,\{[6+4+6+4+9] - 2\,[1+1+2+2+4]\} = 8.
\end{aligned}$$

Appendix

Using a C++ code to compute the sets $A^+(-n)$ for all $1 \leq n \leq 100$ with n square-free, the following table gives the values of $|T^+(-n)|$ and $|\mathcal{O}^G(\mathbb{Q}^*(\sqrt{-n}))|$ for all such n. So that the table fits the page, we denote $|T^+(-n)|$ and $|\mathcal{O}^G(\mathbb{Q}^*(\sqrt{-n}))|$ by $|T^+_{-n}|$ and $|\mathcal{O}^G_{-n}|$, respectively.

n	$\lvert T^+_{-n}\rvert$	$\lvert \mathcal{O}^G_{-n}\rvert$	n	$\lvert T^+_{-n}\rvert$	$\lvert \mathcal{O}^G_{-n}\rvert$	n	$\lvert T^+_{-n}\rvert$	$\lvert \mathcal{O}^G_{-n}\rvert$
1	0	2	33	4	8	67	6	8
2	0	2	34	4	8	69	12	16
3	2	4	35	12	16	70	0	8
5	2	4	37	2	4	71	26	28
6	0	4	38	8	12	73	6	8
7	2	4	39	12	16	74	16	20
10	0	4	41	14	16	77	12	16
11	6	8	42	0	8	78	0	8
13	2	4	43	6	8	79	18	20
14	4	8	46	4	8	82	4	8
15	4	8	47	18	20	83	22	24
17	6	8	51	12	16	85	4	8
19	6	8	53	10	12	86	16	20
21	4	8	55	12	16	87	20	24
22	0	4	57	4	8	89	22	24
23	10	12	59	22	24	91	12	16
26	8	12	61	10	12	93	4	8
29	10	12	62	12	16	94	12	16
30	0	8	65	12	16	95	28	32

31	10	12	66	8	16	97	6	8

Table 2: The number of orbits in $\mathbb{Q}^*(\sqrt{-n})$ for square-free $1 \le n \le 100$

Below is the C++ code used to compute the sets $A^+(-n)$ for $1 \le n \le 100$.

```
#include<iostream> using namespace std;
int main (){
      int n, a, b, c,count = 0,check = 0;
      for (n = 1; n < 101; n++){
            if ((n%4! = 0)&&(n%9! = 0)&&(n%25! = 0)&&(n%49! = 0)){
                  for (a = 1; a < 100; a++){
                        for (b = 2; b < 100; b++){
                              for (c = 2; c < 100; c++){
                                    if ((b > a)&&(c > a)){
                                    if ((b * c − a * a) == n){
                                    cout<<"when n ="<< n <<", a ="<< a <<", b ="
                                                      << b <<", c ="<< c <<endl;
                                                count++;
                                                check= 1;
                                          }
                                    }
                              }
                        }
                  }
                  if (check== 1){
                  cout<<"Possibilities for"<< n <<":"<<count<<endl<<endl;
                        count = 0;
                        check = 0;
                  }
            }
            }
      return 0;
      }
```

Acknowledgement

The authors are deeply grateful to the anonymous referee for his valuable and constructive comments which helped in improving the quality and presentation of the paper. They also extend their appreciation to the Deanship of Scientific Research at King Khalid University for funding this work through the Research Groups Program (grant No. R.G.P2/52/40).

REFERENCES

[1] *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.

[2] *M. Aslam*, Linear Groups and Their Actions on Certain Fields, Ph.D. Thesis, Quaid-i-Azam University, Pakistan, 2004.

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

[4] *L. Ji*, A summary of topics related to group actions, Handbook of Group Actions, Volume 1, Eidtors: L. Ji, A. Papadopoulos, and S-T. Yau, International Press (USA) and Higher Education Press (China), 2015.

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

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

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

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

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

[10] *K. Rosen*, Discrete Mathematics and Its Applications, McGraw-Hill, 7th Edition, 2011.

[11] *A. Torstensson*, Coset diagrams in the study of finitely presented groups with an application to quotients of the modular group, J. Comm. Algebra, **2**(2010), 501-514.