COUNTING CUSPS OF SUBGROUPS OF $\text{PSL}_2(\mathcal{O}_K)$

KATHLEEN L. PETERSEN

Communicated by Ted Chinburg

Abstract. Let $K$ be a number field with $r$ real places and $s$ complex places, and let $\mathcal{O}_K$ be the ring of integers of $K$. The quotient $[\mathbb{H}^2]^r \times [\mathbb{H}^3]^s / \text{PSL}_2(\mathcal{O}_K)$ has $h_K$ cusps, where $h_K$ is the class number of $K$. We show that under the assumption of the generalized Riemann hypothesis that if $K$ is not $\mathbb{Q}$ or an imaginary quadratic field and if $i \not\in K$, then $\text{PSL}_2(\mathcal{O}_K)$ has infinitely many maximal subgroups with $h_K$ cusps. A key element in the proof is a connection to Artin’s Primitive Root Conjecture.

1. Introduction

It is well known that the group of orientation preserving isometries of the hyperbolic plane $\text{Isom}^+(\mathbb{H}^2)$ is isomorphic to $\text{PSL}_2(\mathbb{R})$ and $\text{Isom}^+(\mathbb{H}^3) \cong \text{PSL}_2(\mathbb{C})$. It follows that $\text{PSL}_2(\mathbb{R})^r \times \text{PSL}_2(\mathbb{C})^s$ is isomorphic to the group of orientation preserving isometries of $H_{r,s} = [\mathbb{H}^2]^r \times [\mathbb{H}^3]^s$. If $K$ is a number field with $r$ real places and $s$ complex places and $\mathcal{O}_K$ is the ring of integers of $K$, then $\text{PSL}_2(\mathcal{O}_K)$ embeds discretely in $\text{PSL}_2(\mathbb{R})^r \times \text{PSL}_2(\mathbb{C})^s$ via the map

$$\pm \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \mapsto \prod_{\sigma} \pm \begin{pmatrix} \sigma(\alpha) & \sigma(\beta) \\ \sigma(\gamma) & \sigma(\delta) \end{pmatrix}$$

where the product is taken over all infinite places, $\sigma$ of $K$. The quotient $M_K = H_{r,s}/\text{PSL}_2(\mathcal{O}_K)$ is a finite volume $(2r + 3s)$-dimensional orbifold equipped with a metric inherited from $H_{r,s}$. This orbifold has $h_K$ cusps where $h_K$ is the class number of $K$. If $\Gamma$ is a finite index subgroup of $\text{PSL}_2(\mathcal{O}_K)$, then we let $M_\Gamma = H_{r,s}/\Gamma$. If $M_\Gamma$ has $n$ cusps, we say that $\Gamma$ is $n$-cusped.

The orbifolds $M_K$ have been the focus of much study. The most classical example is $M_\mathbb{Q}$, the quotient of $\mathbb{H}^2$ by the modular group, $\text{PSL}_2(\mathbb{Z})$. It is a hyperbolic 2-orbifold with a single cusp, and is the prototype non-compact arithmetic hyperbolic 2-orbifold. In fact, non-compact arithmetic hyperbolic 2-orbifolds are precisely those hyperbolic 2-orbifolds that are commensurable with $M_\mathbb{Q}$. (Two orbifolds are commensurable if they share a common finite sheeted cover.) Given an imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$ with a ring of integers $\mathcal{O}_d$, the groups $\text{PSL}_2(\mathcal{O}_d)$ are the Bianchi groups, and the corresponding quotients are hyperbolic 3-orbifolds. As in the case of the modular group, the class of all non-compact arithmetic hyperbolic 3-orbifolds consists of those orbifolds commensurable with a quotient of $\mathbb{H}^3$ by a
Bianchi group. When $K$ is totally real, $\text{PSL}_2(\mathcal{O}_K)$ is called the *Hilbert modular group* of $K$. If $K$ is a real quadratic field, the quotient $[\mathbb{H}^2]/\text{PSL}_2(\mathcal{O}_K)$ is a 4-dimensional orbifold, called a *Hilbert modular surface*.

Our result is the following.

**Theorem 1.1.** Let $K$ be a number field other than $\mathbb{Q}$ or an imaginary quadratic field and, in addition, assume that $i \notin K$. Assuming the Generalized Riemann Hypothesis (GRH), there are infinitely many maximal $h_K$-cusped subgroups of $\text{PSL}_2(\mathcal{O}_K)$, where $h_K$ is the class number of $K$.

We show that $\text{PSL}_2(\mathcal{O}_K)$ has infinitely many maximal $h_K$-cusped subgroups if there are infinitely many primes $\mathcal{P}$ in $\mathcal{O}_K$ such that $N_{K/\mathbb{Q}}(\mathcal{P}) \equiv 3 \mod 4$ and $|\mathcal{O}_K^* \mod \mathcal{P}| = |(\mathcal{O}_K/\mathcal{P})^*|$. The GRH is used to prove that there are infinitely many such primes.

The groups $\text{PSL}_2(\mathcal{O}_K)$ have been studied extensively, especially in the context of their normal subgroups. For a non-zero ideal $\mathcal{J} \subset \mathcal{O}_K$, the principal congruence subgroup of level $\mathcal{J}$ is $\Gamma(\mathcal{J}) = \{ A \in \text{PSL}_2(\mathcal{O}_K) : A \equiv I \mod \mathcal{J} \}$. A (finite index) subgroup of $\text{PSL}_2(\mathcal{O}_K)$ is called a congruence subgroup if it contains a principal congruence subgroup. We say that $\text{PSL}_2(\mathcal{O}_K)$ has the congruence subgroup property (CSP) if “almost all” finite index subgroups are congruence subgroups. Precisely, define $\breve{\mathcal{G}}_K$ and $\overline{\mathcal{G}}_K$ as the profinite and congruence completions of $\text{PSL}_2(\mathcal{O}_K)$.

There is an exact sequence

$$\{1\} \rightarrow C_K \rightarrow \breve{\mathcal{G}}_K \rightarrow \overline{\mathcal{G}}_K \rightarrow \{1\},$$

where $C_K$ is called the congruence kernel and measures the prevalence of non-congruence subgroups. Serre [11] proved that $C_K$ is infinite when $K = \mathbb{Q}$ or an imaginary quadratic field. Otherwise, $C_K$ is trivial if $K$ contains a real place, and is isomorphic to the finite cyclic group containing the roots of unity of $K$ if $K$ is totally imaginary.

Rhode [8] proved that for every positive $n$, there are at least two conjugacy classes of one-cusped subgroups of index $n$ in the modular group. Later, Petersson [9] proved that there are only finitely many one-cusped congruence subgroups of the modular group, and that the indices of such groups are the divisors of $55440 = 11 \cdot 7 \cdot 5 \cdot 3^2 \cdot 2^4$. The commutator subgroup of $\text{PSL}_2(\mathbb{Z})$, a subgroup of index 6, is a torsion-free one-cusped congruence subgroup containing $\Gamma(6)$.

Famously, the class number of $\mathbb{Q}(\sqrt{-d})$ is one precisely when $d = 1, 2, 3, 7, 11, 19, 43, 67, \text{or } 163$. These values of $d$ are the only values for which the Bianchi group $\text{PSL}_2(\mathcal{O}_d)$ has one cusp, and consequently such that $\text{PSL}_2(\mathcal{O}_d)$ can contain a one-cusped subgroup. (In contrast, it is a famous conjecture that there are infinitely many real quadratic fields, $K$, with class number one. If this is true, there are infinitely many quotients $[\mathbb{H}^2]/\text{PSL}_2(\mathcal{O}_K)$ with one cusp.) Two notable one-cusped congruence subgroups in $\text{PSL}_2(\mathcal{O}_3)$ are associated to the figure-eight knot and its sister. The fundamental group of the complement of the figure-eight knot in $S^3$ injects as an index 12 subgroup containing $\Gamma(4)$ (see [2]). The fundamental group of the sister of the figure-eight knot complement, a knot in the lens space $L(5,1)$, injects as an index 12 subgroup containing $\Gamma(2)$ (see [1]). Reid [10] has shown that the figure-eight knot complement is the only arithmetic knot complement in $S^3$.

If $d = 2, 7, 11, 19, 43, 67, \text{or } 163$ there are infinitely many maximal one-cusped subgroups of $\text{PSL}_2(\mathcal{O}_d)$, as there is a surjection onto $\mathbb{Z}$ with a parabolic element generating the image. If $d = 1$ or 3 there are infinitely many one-cusped subgroups.
(The fundamental groups of cyclic covers of the figure-eight knot complement all have one cusp.) In contrast, it is shown in [7] that there are only finitely many maximal one-cusped congruence subgroups of the Bianchi groups, and that if \( d = 11, 19, 43, 67, \) or 163 there are only finitely many one-cusped congruence subgroups in \( \text{PSL}_2(\mathcal{O}_d) \). Therefore, we see that especially when the class number is one, Theorem 1.1 further demonstrates the dichotomy between \( \mathbb{Q} \), imaginary quadratic number fields, and other number fields.

There are many examples of one-cusped hyperbolic 2- and 3-manifolds, for example, hyperbolic knot complements in \( \mathbb{P}^3 \). Theorem 1.1 demonstrates the dichotomy between \( \mathbb{Q} \), imaginary quadratic number fields, and other number fields.

Additionally, let \( \Phi_\mathcal{O} \) be the modulo \( \mathcal{O} \) map, followed by the isomorphism from \( \mathcal{O}_K / \mathcal{P} \) to \( \mathbb{F}_q \).

Additionally, let \( \Phi_\mathcal{P} \) be the modulo \( \mathcal{P} \) map, followed by the identification of \( \mathcal{O}_K / \mathcal{P} \) with \( \mathbb{F}_q \) as above:

\[
\Phi_\mathcal{P} : \text{PSL}_2(\mathcal{O}_K) \rightarrow \text{PSL}_2(\mathbb{F}_q).
\]

Notice that \( 0 \notin \Phi_\mathcal{P}(\mathcal{O}_K^\times) \), so we can think of \( \Phi_\mathcal{P} : \mathcal{O}_K^\times \rightarrow \mathbb{F}_q^\times \) where \( \mathbb{F}_q^\times \) is the group of non-zero elements of \( \mathbb{F}_q \).

2. Proof

Before we proceed, we will review some information about peripheral subgroups and cusps. Recall that \( \pm A \in \text{PSL}_2(\mathbb{C}) \) is parabolic if \( \pm A \neq \pm I \) and \( |\text{trace} \ A| = 2 \). Let \( \Gamma \) be a finite index subgroup of \( \text{PSL}_2(\mathcal{O}_K) \). We define \( \mathcal{T} \in \mathbb{C} \cup \infty \) to be a cusp of \( \Gamma \) if \( \mathcal{T} \) is a parabolic fixed point of \( \Gamma \) or if there is a parabolic element \( A \in \Gamma \) such that \( A \cdot \mathcal{T} = \mathcal{T} \) where the action is by linear fractional transformations. For any such \( \mathcal{T} \), we define the corresponding peripheral subgroup as

\[
\text{Stab}_{\mathcal{T}}(\Gamma) = \{ A \in \Gamma : A \cdot \mathcal{T} = \mathcal{T} \}.
\]

Two cusps are equivalent in \( H_{r,s}/\Gamma \) if they are in the same \( \Gamma \) orbit under this action. Each equivalence class corresponds to a conjugacy class of maximal peripheral subgroups of \( \Gamma \) and to a cusp of \( \mathcal{M}_\Gamma \), a finite volume topological end. The orbifold \( \mathcal{M}_K \) has \( h_K \) cusps where \( h_K \) is the class number of \( K \), and hence \( \text{PSL}_2(\mathcal{O}_K) \) has \( h_K \) equivalence classes of cusps. The cusps of \( \text{PSL}_2(\mathcal{O}_K) \) correspond to elements of \( \mathcal{K} \cup \infty \). The equivalence classes of cusps correspond to fractional ideals of \( \mathcal{O}_K \) and with elements of \( \mathbb{P} K^1 \). If \( \mathcal{T} \in \mathcal{K} \) and \( \mathcal{T} = \tau_1 / \tau_2 \) as a reduced fraction, then \( \mathcal{T} \) also corresponds to the fractional ideal generated by \( \tau_1 \) and \( \tau_2^{-1} \) and the element \( (\tau_1 : \tau_2) \in \mathbb{P} K^1 \) (see [13]).

For any \( \mathcal{T} = (t_1 : t_2) \) in \( \mathbb{P} \mathcal{F}_q \), we define

\[
\text{Stab}_{\mathcal{T}}(\text{PSL}_2(\mathcal{F}_q)) = \left\{ \left( \begin{array}{cc} a & b \\ c & d \end{array} \right) : \frac{at_1 + bt_2}{ct_1 + dt_2} = \frac{t_1}{t_2} \right\}.
\]

For a non-zero prime \( \mathcal{P} \) in \( \mathcal{O}_K \) with \( q = N_{K/q}(\mathcal{P}) \), let \( \phi_\mathcal{P} \) be the modulo \( \mathcal{P} \) map, followed by the isomorphism from \( \mathcal{O}_K / \mathcal{P} \) to \( \mathbb{F}_q \):

\[
\phi_\mathcal{P} : \mathcal{O}_K / \mathcal{P} \rightarrow \mathbb{F}_q.
\]

Additionally, let \( \Phi_\mathcal{P} \) be the modulo \( \mathcal{P} \) map, followed by the identification of \( \mathcal{O}_K / \mathcal{P} \) with \( \mathbb{F}_q \) as above:

\[
\Phi_\mathcal{P} : \text{PSL}_2(\mathcal{O}_K) \rightarrow \text{PSL}_2(\mathbb{F}_q).
\]

Notice that \( 0 \notin \Phi_\mathcal{P}(\mathcal{O}_K^\times) \), so we can think of \( \Phi_\mathcal{P} : \mathcal{O}_K^\times \rightarrow \mathbb{F}_q^\times \) where \( \mathbb{F}_q^\times \) is the group of non-zero elements of \( \mathbb{F}_q \).
2.1. Cusps and units. Let $\mathcal{P}$ be a non-zero prime in $\mathcal{O}_K$ of odd norm, $q$. The groups $\text{PSL}_2(F_q)$ always contain a maximal subgroup, $D_{q+1}$, isomorphic to the dihedral group of order $q + 1$ (see [12]). Let

$$\Gamma_{\mathcal{P}} = \Phi_{\mathcal{P}}^{-1}(D_{q+1}).$$

In this section we will prove

**Proposition 2.1.** Let $K$ be a number field, let $\mathcal{P}$ be a prime in $\mathcal{O}_K$ with $q = N_{K/Q}(\mathcal{P})$ and set $l = [F_q^\times : \phi_{\mathcal{P}}(O_K^\times)]$. There is an $M > 2$ such that if $q > M$ and

(i) if $q \equiv 3 \mod 4$, then $\Gamma_{\mathcal{P}}$ has $h_K l$ cusps; otherwise

(ii) if $q \equiv 1 \mod 4$, then $\Gamma_{\mathcal{P}}$ has either $2h_K l$ or $h_K l$ cusps depending on whether or not $D_{q+1}$ contains a non-identity element of the form $\pm \left( \begin{array}{cc} a & 0 \\ 0 & a^{-1} \end{array} \right)$.

This reduces the proof of Theorem [11] to understanding the distribution of the indices $[F_q^\times : \phi_{\mathcal{P}}(O_K^\times)]$ over primes $\mathcal{P}$ in $\mathcal{O}_K$. This will be addressed in the next section. Assuming the following lemma, we will now complete the proof of Proposition 2.1

**Lemma 2.2.** With the notation as above, there is an $M > 2$ such that if $q > M$, then for any cusp $T$ of $\text{PSL}_2(\mathcal{O}_K)$,

$$[\text{Stab}_T(\text{PSL}_2(\mathcal{O}_K)) : \text{Stab}_T(\Gamma(\mathcal{P}))] = q(q-1)/2l.$$

Lemma 2.2 shows that if $q > M$, then all cusps of $M_{\Gamma(\mathcal{P})}$ cover the corresponding cusp of $M_K$ with the same degree. Since $\Gamma(\mathcal{P})$ is a normal subgroup of $\text{PSL}_2(\mathcal{O}_K)$, the number of cusps of $M_{\Gamma(\mathcal{P})}$ covering a single cusp of $M_K$ is

$$\frac{[\text{PSL}_2(\mathcal{O}_K) : \Gamma(\mathcal{P})]}{[\text{Stab}_\infty(\text{PSL}_2(\mathcal{O}_K)) : \text{Stab}_\infty(\Gamma(\mathcal{P}))]} = \frac{\frac{1}{2}q(q-1)}{\frac{1}{2}q(q-1)/l} = l(q+1).$$

Therefore since $\text{PSL}_2(\mathcal{O}_K)$ has $h_K l$ cusps, $\Gamma(\mathcal{P})$ has $h_K l(q+1)$ cusps.

First, assume that $\mathcal{P}$ is as above and additionally that $q \equiv 3 \mod 4$. Since

$$|\text{Stab}_\infty(\text{PSL}_2(F_q))| = \frac{1}{2}q(q-1)$$

and $q \equiv 3 \mod 4$, $\gcd(q(q-1), 2q + 1) = 1$ and we conclude that

$$\text{Stab}_\infty(\text{PSL}_2(F_q)) \cap D_{q+1} = \{id\}.$$

As a result, for any cusp $T$ of $\Gamma_{\mathcal{P}}$, $\text{Stab}_T(\Gamma_{\mathcal{P}}) = \text{Stab}_T(\Gamma(\mathcal{P}))$. Therefore, each cusp of $\Gamma(\mathcal{P})$ covers the corresponding cusp of $\Gamma_{\mathcal{P}}$ with degree one. Since $|\Gamma_{\mathcal{P}} : \Gamma(\mathcal{P})| = q + 1$, the cusp at $\infty$, and hence $T$, is covered by exactly $q + 1$ cusps of $\Gamma(\mathcal{P})$. Therefore $\Gamma_{\mathcal{P}}$ has $h_K l$ cusps.

If $q \equiv 1 \mod 4$, then $\gcd(q(q-1), 2q + 1) = 2$ and therefore

$$|\text{Stab}_\infty(\text{PSL}_2(F_q)) \cap D_{q+1}| = 1 \text{ or } 2.$$

If it is the former, then by the above argument $\Gamma_{\mathcal{P}}$ has $h_K l$ cusps. The latter case occurs precisely when a non-trivial element of the form

$$\pm \left( \begin{array}{cc} a & 0 \\ 0 & a^{-1} \end{array} \right)$$

is in $D_{q+1}$. After conjugation we conclude that for each cusp $T$ of $\Gamma_{\mathcal{P}}$, $|\text{Stab}_T(\Gamma_{\mathcal{P}})| = 2|\text{Stab}_T(\Gamma(\mathcal{P}))|$. Therefore each cusp of $\Gamma(\mathcal{P})$ covers the corresponding cusp of $\Gamma_{\mathcal{P}}$ with degree two and hence $\Gamma_{\mathcal{P}}$ has $2h_K l$ cusps. This proves Proposition 2.1.
Proof of Lemma 2.2. Let \( M > 2 \) be such that if \( q > M \), then for any cusp \( T \) of \( \text{PSL}_2(O_K) \) the parabolic elements in the stabilizer of \( T \) generate a subgroup of order \( q \) modulo \( \mathcal{P} \). Since there are only finitely many equivalence classes of cusps, and all stabilizers in each equivalence class are conjugate, such an \( M \) exists. First, we will prove the lemma for \( T = \infty \). Notice that \( \text{Stab}_\infty(\text{PSL}_2(\mathbb{F}_q)) \) is generated by elements of the form

\[
\pm \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \quad \text{and} \quad \pm \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}
\]

where \( a \in \mathbb{F}_q^\times \) and \( b \in \mathbb{F}_q \). Hence \( |\text{Stab}_\infty(\text{PSL}_2(\mathbb{F}_q))| = q(q-1)/2 \). An element of the second type always has a preimage in \( \text{Stab}_\infty(\text{PSL}_2(O_K)) \), as there is always a \( \beta \in O_K \) such that \( \phi_T(\beta) = b \). An element of the first type has a preimage in \( \text{Stab}_\infty(\text{PSL}_2(O_K)) \) precisely when there is an \( \alpha \in O_K^\times \) mapping to a modulo \( \mathcal{P} \). By hypothesis, \( [\mathbb{F}_q^\times : \phi_T(O_K^\times)] = l \) so \( (q-1)/l \) of the elements in \( \mathbb{F}_q^\times \) have preimages in \( O_K^\times \). As a result, \( (q-1)/2l \) elements of the first type have preimages in \( \text{Stab}_\infty(\text{PSL}_2(O_K)) \). We conclude that \( q(q-1)/2l \) elements of \( \text{Stab}_\infty(\text{PSL}_2(\mathbb{F}_q)) \) have preimages in \( \text{Stab}_\infty(\text{PSL}_2(O_K)) \), establishing that \( |\text{Stab}_\infty(\text{PSL}_2(O_K)) : \text{Stab}_\infty(\Gamma(\mathcal{P}))| = q(q-1)/2l \).

Now we will show the result for \( T \neq \infty \). Let \( (\tau_1 : \tau_2) \) be a representative for \( T \) in \( \mathbb{P}^1 \). We will use \( T \) to denote the fractional ideal generated by \( \tau_1 \) and \( \tau_2^{-1} \) as well. There is an \( \nu \in O_K \) such that \( T^{-1} = \nu^{-1}J \) for some ideal \( J \in O_K \). One can conjugate \( (\tau_1 : \tau_2) \) to \( \infty \) via a matrix of the form

\[
\begin{pmatrix} \tau_1 & \tau_1' \\ \tau_2 & \tau_2' \end{pmatrix}
\]

where \( \tau_1', \tau_2' \in T^{-1} \). Therefore (see [13]) \( \text{Stab}_T(\text{PSL}_2(O_K)) \) is conjugate in \( \text{PSL}_2(K) \) to \( \text{Stab}_\infty(\text{PSL}_2(O_K) \oplus T^{-2}) \), which is

\[
\left\{ \pm \begin{pmatrix} \alpha & \beta \\ 0 & \delta \end{pmatrix} \in \text{PSL}_2(K) : \alpha, \delta \in O_K, \alpha \delta = 1, \beta \in T^{-2} \right\}.
\]

Let \( G(\mathcal{P}) \) be the image of \( \Gamma(\mathcal{P}) \) under this conjugation. Since \( q > M \), \( \text{Stab}_\infty(\text{PSL}_2(O_K) \oplus T^{-2}) \) surjects the parabolic subgroup of \( \text{Stab}_\infty(\text{PSL}_2(\mathbb{F}_q)) \) in the quotient by \( G(\mathcal{P}) \). As in the \( T = \infty \) case,

\[
\left\{ \pm \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} : a \in \mathbb{F}_q^\times \right\}
\]

pulls back to an order \( (q-1)/2l \) subgroup of \( \text{Stab}_\infty(\text{PSL}_2(O_K) \oplus T^{-2}) \). We conclude that \( q(q-1)/2l \) of the elements in \( \text{Stab}_\infty(\text{PSL}_2(\mathbb{F}_q)) \) pull back to elements in \( \text{Stab}_\infty(\text{PSL}_2(O_K) \oplus T^{-2}) \), implying that \( |\text{Stab}_T(\text{PSL}_2(O_K)) : \text{Stab}_T(\Gamma(\mathcal{P}))| = q(q-1)/2l \). \( \square \)

2.2. Artin’s Primitive Root Conjecture. To prove Theorem 1.1 it suffices to prove the following lemma.

Lemma 2.3. Let \( K \) be a number field other than \( \mathbb{Q} \) or an imaginary quadratic field, and, in addition, assume that \( i \not\in K \). Assuming the GRH, there are infinitely many primes \( \mathcal{P} \) in \( O_K \) with \( q = N_K/\mathcal{P} \equiv 3 \mod 4 \) such that \( O_K^\times \) surjects onto \( \mathbb{F}_q^\times \) under the modulo \( \mathcal{P} \) map, i.e., such that \( [\mathbb{F}_q^\times : \phi_\mathcal{P}(O_K^\times)] = 1 \).

Together with Proposition 2.1 this proves Theorem 1.1. The generalized Riemann hypothesis assumed is as follows, as required in [3].
Assumption. For all square-free \( n > 0 \) the Dedekind zeta function of \( L_{n,1} \) satisfies the generalized Riemann hypothesis, where \( L_{n,1} \) is the field obtained by adjoining to \( K \) the \( q_l(n) \)th roots of elements in \( \mathcal{O}_K^\times \). We define \( q_l(n) \) as follows:

\[
q_l(n) = \prod_{r|n} q_l(r),
\]

where the product is taken over all primes \( r \) dividing \( n \) and \( q_l(r) \) is the smallest power of \( r \) not dividing \( l \).

The condition that we require in Lemma 2.3 is closely related to Artin’s Primitive Root Conjecture, which we will now state.

Conjecture 2.4 (Artin). Let \( b \) be an integer other than \(-1\) or a square. There are infinitely many primes, \( p \), such that \( b \) generates the multiplicative group modulo \( p \), i.e. such that \( [\mathbb{F}_p^\times : \phi_p(b)] = 1 \).

Hooley [3] proved the above conjecture under the assumption of the generalized Riemann hypothesis. Weinberger [14] generalized Hooley’s conditional proof to the number field setting, and later Lenstra [5] refined this work. Unconditionally, if \( K \) is Galois with unit rank greater than \( 3 \), techniques of Murty and Harper [2] imply that there are infinitely many primes \( \mathcal{P} \) such that \( \mathcal{O}_K^\times \) surjects the multiplicative group modulo \( \mathcal{P} \). Therefore we have the following, unconditionally.

Theorem 2.5. If \( K \) is Galois with unit rank greater than \( 3 \), there are infinitely many maximal subgroups of \( \text{PSL}_2(\mathcal{O}_K) \) with either \( h_K \) or \( 2h_K \) cusps.

We will make use of [5], Theorem 3.1. First, we establish some notation. If \( F \) is a Galois extension of \( K \), recall that the Artin symbol \( (\mathcal{P}, F/K) \) denotes the set of \( \sigma \in \text{Gal}(F/K) \) for which there is a prime \( \mathcal{Q} \) in \( F \) lying over \( \mathcal{P} \) such that \( \sigma(\mathcal{Q}) = \mathcal{Q} \) and \( \sigma(a) \equiv a^q \mod \mathcal{Q} \) where \( q = N_{K/\mathcal{Q}}(\mathcal{P}) \). Following [5], for \( F \) a Galois extension of \( K, C \) a subset of \( \text{Gal}(F/K) \), \( W \) a finitely generated subgroup of \( K^\times \), and \( l \) a positive integer, let \( M(K, F, C, W, l) \) denote those primes \( \mathcal{P} \) of \( K \) which satisfy \( (\mathcal{P}, F/K) \subset C, \text{ord}_\mathcal{P}(w) = 0 \) for all \( w \in W \), and such that \( [\mathbb{F}_q^\times : \phi_\mathcal{P}(\mathcal{O}_K^\times)] \) is divisible by \( l \). Let \( \mu \) be the Möbius function

\[
\mu(n) = \begin{cases} 
0 & \text{if } n \text{ has one or more repeated prime divisors}, \\
1 & \text{if } n = 1, \\
(-1)^k & \text{if } n \text{ is a product of } k \text{ distinct primes},
\end{cases}
\]

and let \( c(n, l, C) = |C \cap \text{Gal}(F/(F \cap L_{n,l}))| \). Define

\[
D(K, F, C, W, l) = \sum_n \frac{\mu(n)c(n, l, C)}{|F : L_{n,l} : K|},
\]

where \( L_{n,l} \) is the field obtained by adjoining to \( K \) the \( q_l(n) \)th roots of elements in \( W \). Assuming the GRH, it is shown in [5] that \( M(K, F, C, W, l) \) has a natural density equal to \( D(K, F, C, W, l) \).

Proof of Lemma 2.3. The set \( M(K, K(i), \{\sigma\}, \mathcal{O}_K^\times, 1) \) is the set of unramified primes \( \mathcal{P} \) with \( q = N_{K/\mathcal{Q}}(\mathcal{P}) \equiv 3 \mod 4 \) such that \( [\mathbb{F}_q^\times : \phi_\mathcal{P}(\mathcal{O}_K^\times)] = 1 \). Since \( i \notin K \), the stipulation that \( (\mathcal{P}, K(i)/K) = \{\sigma\} \) corresponds to the norm being congruent to \( 3 \mod 4 \). The stipulation that \( l = 1 \) is the condition that \( [\mathbb{F}_q^\times : \phi_\mathcal{P}(\mathcal{O}_K^\times)] = 1 \).
It follows from the conditions in [5] that $D(K, K(i), \{\sigma\}, \mathcal{O}_K^\times, 1)$ is positive when $K$ is a number field other than $\mathbb{Q}$ or an imaginary quadratic number field, $i \not\in K$, and $\sigma$ is complex conjugation. In fact, if $r$ is the rank of $\mathcal{O}_K^\times$,

$$D(K, K(i), \{\sigma\}, \mathcal{O}_K^\times, 1) = \left(1 - \frac{1}{2^r}\right) \sum_{n} \frac{\mu(n)}{[L_{n,1} : K]}$$

$$= \left(1 - \frac{1}{2^r}\right) D(K, K, \{\text{id}\}, \mathcal{O}_K^\times, 1),$$

where $D(K, K, \{\text{id}\}, \mathcal{O}_K^\times, 1)$ is the previous density without the congruence condition. 

\[\square\]

Acknowledgements

This paper is an extension of part of the author’s doctoral thesis [6]. The author would like to thank her advisor, Alan Reid, for his guidance and support.

References


Department of Mathematics and Statistics, Queen’s University, Kingston, Ontario K7L 3N6, Canada

E-mail address: petersen@math.queensu.ca