PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 136, Number 7, July 2008, Pages 2387–2393
S 0002-9939(08)09262-9
Article electronically published on March 14, 2008

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

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 $[\mathbb{H}^2]^r \times [\mathbb{H}^3]^s/\mathrm{PSL}_2(\mathcal{O}_K)$ 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 $i \notin K$, then $\mathrm{PSL}_2(\mathcal{O}_K)$ 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 $\mathrm{Isom}^+(\mathbb{H}^2)$ is isomorphic to $\mathrm{PSL}_2(\mathbb{R})$ and $\mathrm{Isom}^+(\mathbb{H}^3) \cong \mathrm{PSL}_2(\mathbb{C})$. It follows that $\mathrm{PSL}_2(\mathbb{R})^r \times \mathrm{PSL}_2(\mathbb{C})^s$ 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 $\mathrm{PSL}_2(\mathcal{O}_K)$ embeds discretely in $\mathrm{PSL}_2(\mathbb{R})^r \times \mathrm{PSL}_2(\mathbb{C})^s$ 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, σ of K. The quotient $M_K = H_{r,s}/\mathrm{PSL}_2(\mathcal{O}_K)$ 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 Γ is a finite index subgroup of $\mathrm{PSL}_2(\mathcal{O}_K)$, then we let $M_\Gamma = H_{r,s}/\Gamma$. If M_Γ has n cusps, we say that Γ 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,* $\mathrm{PSL}_2(\mathbb{Z})$. 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 $\mathrm{PSL}_2(\mathcal{O}_d)$ 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

Received by the editors June 5, 2006, and, in revised form, July 12, 2006, November 28, 2006, and June 11, 2007.
2000 *Mathematics Subject Classification.* Primary 11F23, 22E40, 11A07.

©2008 American Mathematical Society
Reverts to public domain 28 years from publication

Bianchi group. When K is totally real, $\mathrm{PSL}_2(\mathcal{O}_K)$ is called the *Hilbert modular group* of K. If K is a real quadratic field, the quotient $[\mathbb{H}^2]^2/\mathrm{PSL}_2(\mathcal{O}_K)$ 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 $\mathrm{PSL}_2(\mathcal{O}_K)$, where h_K is the class number of K.*

We show that $\mathrm{PSL}_2(\mathcal{O}_K)$ 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 $|\mathcal{O}_K^\times \mod \mathcal{P}| = |(\mathcal{O}_K/\mathcal{P})^\times|$. The GRH is used to prove that there are infinitely many such primes.

The groups $\mathrm{PSL}_2(\mathcal{O}_K)$ 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 $\Gamma(\mathcal{J}) = \{A \in \mathrm{PSL}_2(\mathcal{O}_K) : A \equiv I \mod \mathcal{J}\}$. A (finite index) subgroup of $\mathrm{PSL}_2(\mathcal{O}_K)$ is called a *congruence subgroup* if it contains a principal congruence subgroup. We say that $\mathrm{PSL}_2(\mathcal{O}_K)$ has the *congruence subgroup property (CSP)* if "almost all" finite index subgroups are congruence subgroups. Precisely, define $\widehat{G_K}$ and $\overline{G_K}$ as the profinite and congruence completions of $\mathrm{PSL}_2(\mathcal{O}_K)$. There is an exact sequence

$$\{1\} \to C_K \to \widehat{G_K} \to \overline{G_K} \to \{1\},$$

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 $\mathrm{PSL}_2(\mathbb{Z})$, 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, or 163. These values of d are the only values for which the Bianchi group $\mathrm{PSL}_2(\mathcal{O}_d)$ has one cusp, and consequently such that $\mathrm{PSL}_2(\mathcal{O}_d)$ 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 $[\mathbb{H}^2]^2/\mathrm{PSL}_2(\mathcal{O}_K)$ with one cusp.) Two notable one-cusped congruence subgroups in $\mathrm{PSL}_2(\mathcal{O}_3)$ 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 [4]). 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, or 163 there are infinitely many maximal one-cusped subgroups of $\mathrm{PSL}_2(\mathcal{O}_d)$, 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 $\mathrm{PSL}_2(\mathcal{O}_d)$. 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 S^3. As commented, the commutator subgroup of the modular group is torsion-free and has one-cusp. Additionally, the figure-eight knot complement and sister are one-cusped manifolds. However, the groups considered in the proof of Theorem 1.1 all necessarily contain torsion. In fact, there are no known examples of one-cusped hyperbolic n-manifolds for $n \geq 4$, or of torsion-free subgroups of $\mathrm{PSL}_2(\mathcal{O}_K)$ whose quotients have finite volume and only one cusp when $K \neq \mathbb{Q}$ or has an imaginary quadratic field.

2. Proof

Before we proceed, we will review some information about peripheral subgroups and cusps. Recall that $\pm A \in \mathrm{PSL}_2(\mathbb{C})$ is *parabolic* if $\pm A \neq \pm I$ and $|\text{trace } A| = 2$. Let Γ be a finite index subgroup of $\mathrm{PSL}_2(\mathcal{O}_K)$. We define $\mathcal{T} \in \mathbb{C} \cup \infty$ to be a *cusp* of Γ if $\mathcal{T}$ is a parabolic fixed point of Γ 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

$$\mathrm{Stab}_{\mathcal{T}}(\Gamma) = \{A \in \Gamma : A \cdot \mathcal{T} = \mathcal{T}\}.$$

Two cusps are equivalent in $H_{r,s}/\Gamma$ if they are in the same Γ orbit under this action. Each equivalence class corresponds to a conjugacy class of maximal peripheral subgroups of Γ and to a cusp of M_Γ, a finite volume topological end. The orbifold M_K has h_K cusps where h_K is the class number of K, and hence $\mathrm{PSL}_2(\mathcal{O}_K)$ has h_K equivalence classes of cusps. The cusps of $\mathrm{PSL}_2(\mathcal{O}_K)$ correspond to elements of $K \cup \infty$. The equivalence classes of cusps correspond to fractional ideals of $\mathcal{O}_K$ and with elements of $\mathbb{P}K^1$. If $\mathcal{T} \in K$ and $\mathcal{T} = \tau_1/\tau_2$ as a reduced fraction, then $\mathcal{T}$ also corresponds to the fractional ideal generated by τ_1 and τ_2^{-1} and the element $(\tau_1 : \tau_2) \subset \mathbb{P}K^1$ (see [13]).

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

$$\mathrm{Stab}_T(\mathrm{PSL}_2(\mathbb{F}_q)) = \left\{ \pm \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \frac{at_1 + bt_2}{ct_1 + dt_2} = \frac{t_1}{t_2} \right\}.$$

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

$$\phi_{\mathcal{P}} : \mathcal{O}_K \to \mathbb{F}_q.$$

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

$$\Phi_{\mathcal{P}} : \mathrm{PSL}_2(\mathcal{O}_K) \to \mathrm{PSL}_2(\mathbb{F}_q).$$

Notice that $0 \notin \phi_{\mathcal{P}}(\mathcal{O}_K^\times)$, so we can think of $\phi_{\mathcal{P}} : \mathcal{O}_K^\times \to \mathbb{F}_q^\times$ 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 $\mathrm{PSL}_2(\mathbb{F}_q)$ 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 $q = N_{K/\mathbb{Q}}(\mathcal{P})$ and set $l = [\mathbb{F}_q^\times : \phi_{\mathcal{P}}(\mathcal{O}_K^\times)]$. There is an $\mathcal{M} > 2$ such that if $q > \mathcal{M}$ 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 $\pm \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$.

This reduces the proof of Theorem 1.1 to understanding the distribution of the indices $[\mathbb{F}_q^\times : \phi_{\mathcal{P}}(\mathcal{O}_K^\times)]$ 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 $\mathcal{M} > 2$ such that if $q > \mathcal{M}$, then for any cusp $\mathcal{T}$ of $\mathrm{PSL}_2(\mathcal{O}_K)$,*

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

Lemma 2.2 shows that if $q > \mathcal{M}$, 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 $\mathrm{PSL}_2(\mathcal{O}_K)$, the number of cusps of $M_{\Gamma(\mathcal{P})}$ covering a single cusp of M_K is

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

Therefore since $\mathrm{PSL}_2(\mathcal{O}_K)$ has h_K 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

$$|\mathrm{Stab}_\infty(\mathrm{PSL}_2(\mathbb{F}_q))| = \frac{1}{2}q(q-1)$$

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

$$\mathrm{Stab}_\infty(\mathrm{PSL}_2(\mathbb{F}_q)) \cap D_{q+1} = \{id\}.$$

As a result, for any cusp $\mathcal{T}$ of $\Gamma_{\mathcal{P}}$, $\mathrm{Stab}_{\mathcal{T}}(\Gamma_{\mathcal{P}}) = \mathrm{Stab}_{\mathcal{T}}(\Gamma(\mathcal{P}))$. 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 ∞, and hence $\mathcal{T}$, 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 $\gcd(q(q-1)/2, q+1) = 2$ and therefore

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

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

$$\pm \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$$

is in D_{q+1}. After conjugation we conclude that for each cusp $\mathcal{T}$ of $\Gamma_{\mathcal{P}}$, $|\mathrm{Stab}_{\mathcal{T}}(\Gamma_{\mathcal{P}})| = 2|\mathrm{Stab}_{\mathcal{T}}(\Gamma(\mathcal{P}))|$. 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 $\mathcal{M} > 2$ be such that if $q > \mathcal{M}$, then for any cusp $\mathcal{T}$ of $\mathrm{PSL}_2(\mathcal{O}_K)$ the parabolic elements in the stabilizer of $\mathcal{T}$ 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 $\mathcal{M}$ exists. First, we will prove the lemma for $\mathcal{T} = \infty$. Notice that $\mathrm{Stab}_\infty(\mathrm{PSL}_2(\mathbb{F}_q))$ is generated by elements of the form

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

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

Now we will show the result for $\mathcal{T} \neq \infty$. Let $(\tau_1 : \tau_2)$ be a representative for $\mathcal{T}$ in $\mathbb{P}K^1$. We will use $\mathcal{T}$ to denote the fractional ideal generated by τ_1 and τ_2^{-1} as well. There is an $\nu \in \mathcal{O}_K$ such that $\mathcal{T}^{-1} = \nu^{-1}\mathcal{J}$ for some ideal $\mathcal{J} \in \mathcal{O}_K$. One can conjugate $(\tau_1 : \tau_2)$ to ∞ via a matrix of the form

$$A_\mathcal{T} = \pm\begin{pmatrix} \tau_1 & \tau_1' \\ \tau_2 & \tau_2' \end{pmatrix}$$

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

$$\left\{\pm\begin{pmatrix} \alpha & \beta \\ 0 & \delta \end{pmatrix} \in \mathrm{PSL}_2(K) : \alpha, \delta \in \mathcal{O}_K, \alpha\delta = 1, \beta \in \mathcal{T}^{-2}\right\}.$$

Let $G(\mathcal{P})$ be the image of $\Gamma(\mathcal{P})$ under this conjugation. Since $q > \mathcal{M}$, $\mathrm{Stab}_\infty(\mathrm{PSL}_2(\mathcal{O}_K) \oplus \mathcal{T}^{-2})$ surjects the parabolic subgroup of $\mathrm{Stab}_\infty(\mathrm{PSL}_2(\mathbb{F}_q))$ in the quotient by $G(\mathcal{P})$. As in the $\mathcal{T} = \infty$ 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 $\mathrm{Stab}_\infty(\mathrm{PSL}_2(\mathcal{O}_K) \oplus \mathcal{T}^{-2})$. We conclude that $q(q-1)/2l$ of the elements in $\mathrm{Stab}_\infty(\mathrm{PSL}_2(\mathbb{F}_q))$ pull back to elements in $\mathrm{Stab}_\infty(\mathrm{PSL}_2(\mathcal{O}_K) \oplus \mathcal{T}^{-2})$, implying that $[\mathrm{Stab}_\mathcal{T}(\mathrm{PSL}_2(\mathcal{O}_K)) : \mathrm{Stab}_\mathcal{T}(\Gamma(\mathcal{P}))] = q(q-1)/2l$. □

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 $i \notin K$. Assuming the GRH, there are infinitely many primes $\mathcal{P}$ in $\mathcal{O}_K$ with $q = N_{K/\mathbb{Q}}(\mathcal{P}) \equiv 3 \mod 4$ such that $\mathcal{O}_K^\times$ surjects onto $\mathbb{F}_q^\times$ under the modulo $\mathcal{P}$ map, i.e. such that $[\mathbb{F}_q^\times : \phi_\mathcal{P}(\mathcal{O}_K^\times)] = 1$.*

Together with Proposition 2.1 this proves Theorem 1.1. The generalized Riemann hypothesis assumed is as follows, as required in [5].

Assumption. *For all square-free $n > 0$ the Dedekind zeta function of $L_{n,l}$ satisfies the generalized Riemann hypothesis, where $L_{n,l}$ is the field obtained by adjoining to K the $q_l(n)^{\text{th}}$ 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 $[\mathbb{F}_p^\times : \phi_p(\langle b\rangle)] = 1$.*

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 $\mathrm{PSL}_2(\mathcal{O}_K)$ 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 $\sigma \in \mathrm{Gal}(F/K)$ for which there is a prime $\mathcal{Q}$ in F lying over $\mathcal{P}$ such that $\sigma(\mathcal{Q}) = \mathcal{Q}$ and $\sigma(\alpha) \equiv \alpha^q \mod \mathcal{Q}$ where $q = N_{K/\mathbb{Q}}(\mathcal{P})$. Following [5], for F a Galois extension of K, C a subset of $\mathrm{Gal}(F/K)$, 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 $(\mathcal{P}, F/K) \subset C$, $ord_{\mathcal{P}}(w) = 0$ for all $w \in W$, and such that $[\mathbb{F}_q^\times : \phi_{\mathcal{P}}(\mathcal{O}_K^\times)]$ is divisible by l. Let μ 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 $c(n,l,C) = |C \cap \mathrm{Gal}(F/(F \cap L_{n,l}))|$. Define

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

where $L_{n,l}$ is the field obtained by adjoining to K the $q_l(n)^{\text{th}}$ 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 $q = N_{K/\mathbb{Q}}(\mathcal{P}) \equiv 3 \mod 4$ 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, $i \notin K$, and σ is complex conjugation. In fact, if $\mathfrak{r}$ is the rank of $\mathcal{O}_K^\times$,

$$\begin{aligned} D(K, K(i), \{\sigma\}, \mathcal{O}_K^\times, 1) &= \left(1 - \frac{1}{2^{\mathfrak{r}}}\right) \sum_n \frac{\mu(n)}{[L_{n,l} : K]} \\ &= \left(1 - \frac{1}{2^{\mathfrak{r}}}\right) D(K, K, \{\mathrm{id}\}, \mathcal{O}_K^\times, 1), \end{aligned}$$

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

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

1. M. D. Baker and A. W. Reid, *Arithmetic knots in closed 3-manifolds*, J. Knot Theory Ramifications **11** (2002), no. 6, 903–920, Knots 2000 Korea, Vol. 3 (Yongpyong). MR1936242 (2004b:57009)
2. M. Harper and M. R. Murty, *Euclidean rings of algebraic integers*, Canad. J. Math. **56** (2004), no. 1, 71–76. MR2031123 (2005h:11261)
3. C. Hooley, *On Artin's conjecture*, J. Reine Angew. Math. **225** (1967), 209–220. MR0207630 (34:7445)
4. C. J. Leininger, *Compressing totally geodesic surfaces*, Topology Appl. **118** (2002), no. 3, 309–328. MR1874553 (2002j:57017)
5. H. W. Lenstra, Jr., *On Artin's conjecture and Euclid's algorithm in global fields*, Invent. Math. **42** (1977), 201–224. MR0480413 (58:576)
6. K. L. Petersen, *One-cusped congruence subgroups of* $\mathrm{PSL}_2(\mathcal{O}_k)$, University of Texas at Austin, 2005, Doctoral Thesis.
7. ———, *One-cusped congruence subgroups of Bianchi groups*, Math. Ann. **338** (2007), no. 2, 249–282. MR2302062
8. H. Petersson, *Über einen einfachen Typus von Untergruppen der Modulgruppe*, Arch. Math. **4** (1953), 308–315. MR0057910 (15,291a)
9. ———, *Über die Konstruktion zykloider Kongruenzgruppen in der rationalen Modulgruppe*, J. Reine Angew. Math. **250** (1971), 182–212. MR0294255 (45:3324)
10. A. W. Reid, *Arithmeticity of knot complements*, J. London Math. Soc. (2) **43** (1991), no. 1, 171–184. MR1099096 (92a:57011)
11. J.-P. Serre, *Le problème des groupes de congruence pour SL2*, Ann. of Math. (2) **92** (1970), 489–527. MR0272790 (42:7671)
12. M. Suzuki, *Group theory. I*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 247, Springer-Verlag, Berlin, 1982, Translated from the Japanese by the author. MR648772 (82k:20001c)
13. G. van der Geer, *Hilbert modular surfaces*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 16, Springer-Verlag, Berlin, 1988. MR930101 (89c:11073)
14. P. J. Weinberger, *On Euclidean rings of algebraic integers*, Analytic number theory (Proc. Sympos. Pure Math., Vol. XXIV, St. Louis Univ., St. Louis, Mo., 1972), Amer. Math. Soc., Providence, R. I., 1973, pp. 321–332. MR0337902 (49:2671)

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

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